Detection Copy-Move Forgery in Image Via Quaternion Polar Harmonic Transforms

Salam A. Thajeel[1*], Ali Shakir Mahmood[1], Waleed Rasheed Humood[1] & Ghazali Sulong[2]
[1]Computer Science Department, College of Education, Mustansiriyah University, Baghdad, Iraq
[2]Universiti Malaysia Terengganu, 21030, Kuala Terengganu, Malaysia
[dr.salam.thajeel@uomustansiriyah.edu.iq, asmjhm2006@uomustansiriyah.edu.iq, waleed77@uomustansiriyah.edu.iq, ghazali.s@umt.edu.my]
*Corresponding author: Salam A. Thajeel

Received June 18, 2018; revised December 11, 2018; revised January 28, 2019; accepted February 22, 2019; published August 31, 2019

Abstract

Copy–move forgery (CMF) in digital images is a detrimental tampering of artefacts that requires precise detection and analysis. CMF is performed by copying and pasting a part of an image into other portions of it. Despite several efforts to detect CMF, accurate identification of noise, blur and rotated region-mediated forged image areas is still difficult. A novel algorithm is developed on the basis of quaternion polar complex exponential transform (QPCET) to detect CMF and is conducted involving a few steps. Firstly, the suspicious image is divided into overlapping blocks. Secondly, invariant features for each block are extracted using QPCET. Thirdly, the duplicated image blocks are determined using k-dimensional tree (kd-tree) block matching. Lastly, a new technique is introduced to reduce the flat region-mediated false matches. Experiments are performed on numerous images selected from the CoMoFoD database. MATLAB 2017b is used to employ the proposed method. Metrics such as correct and false detection ratios are utilised to evaluate the performance of the proposed CMF detection method. Experimental results demonstrate the precise and efficient CMF detection capacity of the proposed approach even under image distortion including rotation, scaling, additive noise, blurring, brightness, colour reduction and JPEG compression. Furthermore, our method can solve the false match problem and outperform existing ones in terms of precision and false positive rate. The proposed approach may serve as a basis for accurate digital image forensic investigations.

***Keywords*:** Copy move forgery detection (CMFD); duplicated region detection; feature extraction; digital image forensic; QPCET.

1. Introduction

In the present information communication technology era, images are considered fundamental tools for effective information exchange. Images as information source (serving as official document) play an important role in criminal and forensic investigations. Rapid advancement in digital image processing technology in terms of hardware (digital cameras) and software (image editing applications) has made manipulation easily feasible. Image contents can easily be tainted by adding or removing some essential elements to create a misleading image without leaving observable signatures [1]. This manipulation or counterfeiting is invisible to the human eye. Thus, image originality authentication is challenging. New tools and techniques to ensure image legitimacy and integrity are created.

Recently, digital forgery detection is introduced to address this issue and emerges as an important field in image processing [2]. Digital forgery detection techniques are classified into active and passive (blind) [3]. Active approach embeds data or digital signature into original images via pre-processing, thereby limiting its practical applications. Numerous digital images exist in the Internet without any prior information or digital signature and watermark [4].

Conversely, passive method does not require any extra data for embedment. The performance of this method is based on the absence of any data and signature during digitising. Most passive techniques verify image integrity through analysis of image statistics and properties, including sensor noise and illumination conditions [5]. Passive detection approaches are popular and widely applied and aim to solve some special tampering attempts.

However, a unique detection technique that deals with all types of forgeries is still yet to be discovered [5]. Image forgery has different types. Digital images are popularly manipulated using three forgery mechanisms: copy–move (cloning), image splicing and image retouching. The simplicity of copy–move or cloning forgery makes it a basic and familiar image manipulation scheme [6]. In copy–move forgery (CMF), a part of an image is copied and pasted to another location of it to cancel or duplicate valuable information [7].

Most professional forgers normally hide traces of forgeries by applying some forms of attacks such as photometric manipulation and geometric transformation. Such attacks generate seamlessly integrated images, thereby making forgery detection visually impossible and technically challenging [7]. JPEG compression, Gaussian noise, blurring, brightness adjustment and colour reduction are commonly used photometric manipulation techniques, whereas rotation and scaling represent geometric transformation. Thus, CMF detection (CMFD) technique should be robust to rotation, blurring, noise and compression [8].

A robust CMFD scheme is proposed on the basis of quaternion polar complex exponential transform (QPCET) [9] to authenticate image originality. This study contributes to literature by selecting QPCET and making it a local feature in block-based technique. This work also improves the implementation of random sample consensus (RANSAC) by reducing false matching to increase efficiency. The performance of the proposed method in terms of detection accuracy is compared with that of existing methods. The said method not only detects the tampered image region precisely but also is robust against rotation, scaling, JPEG compression, blurring and noise inclusion.

The rest of the paper is organised as follows. Section 2 briefly reviews CMFD methods. Section 3 describes development of the proposed CMFD method. Section 4 presents the experimental design in detail with important results and the performance evaluation of the

proposed method in terms of detection accuracy. Section 5 shows the discussion of results. Section 6 presents the conclusions and upcoming outlook.

2. Related Work

Numerous techniques have been recently proposed for CMFD. They can be classified in two: block and key point matching. In the former category, the image is firstly segmented into small overlapping or non-overlapping blocks to extract each block feature. Then, these blocks are compared for matching [10]. Discussing the advantages and disadvantages of existing block-based CMFD techniques is relevant. Fridrich et al. [11] firstly proposed a block-based method in which the discrete cosine transform (DCT) is used to extract the coefficient for each overlapping block. The detected duplicated regions depend on matching the quantisation coefficient that is lexicographically sorted. This method exhibits poor robustness and high computing complexity. Popescu and Farid [12] introduced a similar method by replacing DCT with principal component analysis. Despite its great effectiveness, this method still fails to detect copied regions that are rotated prior to pasting. Many efforts have been made for CMFD using DCT [13–15]. Mahdian and Saic [16] used the blur moment invariant to detect copy–move region for exposed image containing blurs or added noise. This method also fails to detect the forged area after being rotated or flipped.

Li [17] used local binary pattern (LBP) for CMFD. In this method, the image is divided into overlapping circular blocks and filtered using a low-pass filter before LBP is applied for further extraction of features. Polar harmonic transform is then adopted [18] to describe circular block contents. Superior results are achieved for images exposed with simple additive noise and JPEG compression, and the method is robust to region rotation and flipping. However, this method cannot detect images exposed to random region rotations. Zhong, J., et al. [19] offered a new block-based technique for CMF. In this technique, the suspicion image is divided into overlapped circular blocks, and local and inner image features are extracted using discrete radial harmonic Fourier coefficients. 2 nearest neighbours, Euclidean distance and correlation coefficient are implemented to identify the forged regions amongst image blocks. Morphological operation is used to delete the isolated pixels. Forgery is identified from the pixel information.

Hosny et al. [20] proposed a new method for CMFD based on a new framework. In this method, the duplicated object is enclosed in a bounding box and treated as a sub-image. Therefore, the computation time of the feature extraction step here is for calculating the features for the segmented objects only and not for the entire image similar to all the common methods used before. In addition, accurate PCET is used to achieve accurate detection results. The experimental results showed that the proposed method exhibits excellent robustness to various post-processing operations, such as adding white Gaussian noise, JPEG compression, rotation and scaling.

Mahmood, T. et al. [21] presented a new block-based technique for CMF based on stationary wavelet transform (SWT) and DCT. In this technique, the suspicious image is converted into YCbCr colour space. Then, the image is decomposed into four sub-bands (approximation, horizontal, vertical and diagonal) via SWT. Thereafter, the approximation sub-band is divided into overlapping blocks and DCT is used on these blocks. The experimental results indicated that the proposed technique has high accuracy even when the forged image is exposed to some post-processing attacks.

Key point-based methods are different from block-based methods because they do not divide images into blocks to extract features. The former extracts feature from regions

around the previously determined key point (key point detector). A few approaches such as scale invariant feature transform (SIFT) [22], SURF [23] and ORB [24] are developed to extract interest points. Huang et al. [22] proposed SIFT for CMFD. Amerini [25] improved the SIFT approach by incorporating hierarchical clustering to the key points to successfully filter the key points into few classes.

Bo et al. [23] introduced a CMFD method based on SURF. This method can detect duplicated regions of different sizes with the minimum number of false matches in dealing with high-resolution images. Hen et al. [26] used Harris corner interest points to extract image key points and step sector statistics to represent small circular image regions around each Harris point using a feature vector. Yang, Li et al. [27] suggested a novel method based on hybrid feature. In this method, a powerful interest point detector called KAZE is introduced and combined with SIFT to extract feature points for detecting forgery in smooth regions. The experimental results showed that this method can detect multiple duplicated regions due to the improved n-best matching scheme. An efficient filtering based on iterative strategy has also been used to reduce false matching. The outcomes exhibited that the proposed strategy can detect forge region even under distortions. Some key points in duplicate regions can be identified using key point-based algorithms. Copied regions with little textural structure may be missed entirely. Key point-based methods are also prone to several post-processing operations, including blurring and flipping. Both methods reveal strengths and weaknesses. Block-matching techniques are effective for forgery detection and robust to JPEG compression, blurring or additive noise. To date, only few methods are effective and robust against geometrical attacks such as rotation, scaling and distortion. Sift-matching techniques possess some limitations on detection performance because they extract image key points from peculiar points only. Most of the mentioned methods are evaluated against single attacks only.

3. Proposed Detection Method

Suitable and robust feature extraction from blocks is a prerequisite to ensure efficient detection. These features must be robust against geometric (rotation and scaling) and photometric attacks (noise, blur and brightness) with reduced false matching. **Fig. 1** presents the framework of the proposed scheme. The test colour image is firstly partitioned to overlapping circular blocks and then in each block. Secondly, QPCET is applied on each block to extract features. Three feature vectors will be obtained for each block (one for each colour channel). Thirdly, the block matching is performed in two stages: sorting and searching. This study adopts the k-dimensional tree (KD-tree) algorithm for the former, whereas the approximate nearest neighbour is employed for the latter. Lastly, we reduce the false matches using RANSAC. The details of these processes are explained in detail in Sections 3.1–3.4.

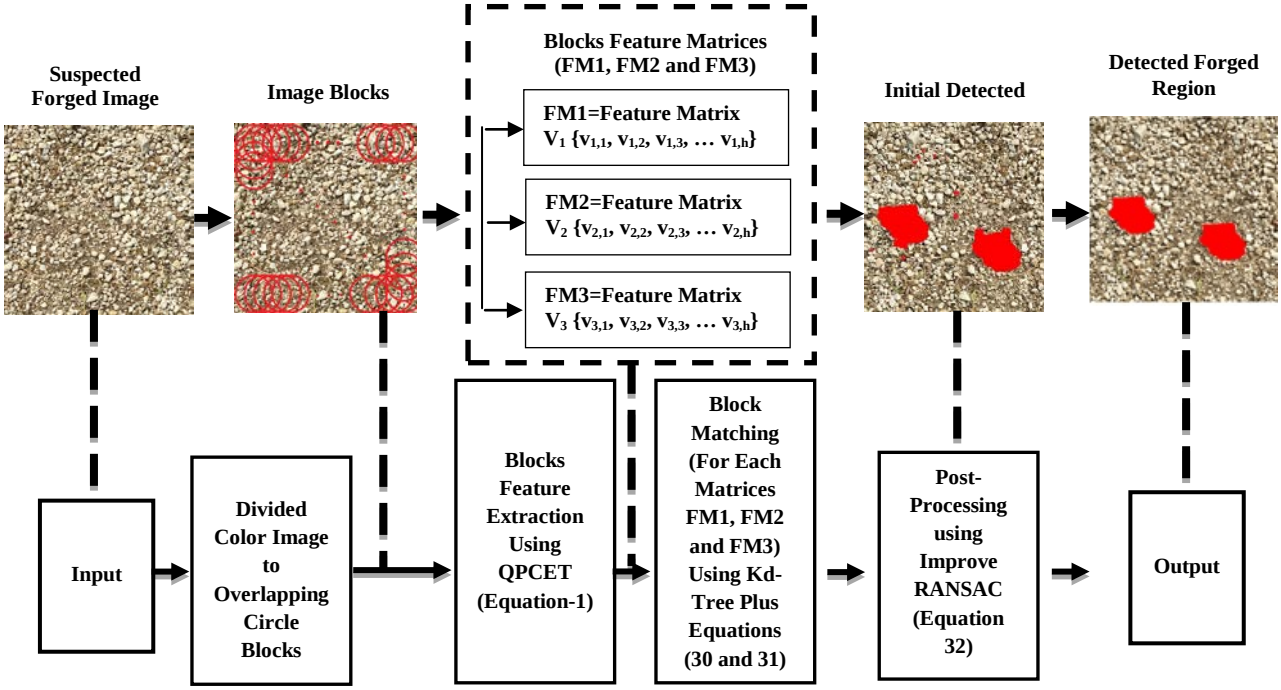


Fig. 1. Framework of the proposed copy–move forgery detection scheme.

3.1 Block Tilling

Unlike numerous existing techniques of image pre-processing, converting colour image to grey scale is no longer necessary in the proposed method because QPCET is used as a feature descriptor to handle colour images.

A colour image is used as input image in the first step of the proposed CMFD method. The suspected image is usually divided into overlapping blocks to extract features from these blocks for determining forged regions. Most of the present schemes use square blocks. However, the suspected image (colour image) in the proposed method is divided into overlapping circular blocks to determine forged regions. The reason is that the circular shape of block is designed to reduce the block border effects that influence the detection result and is suitable for QPCET in computing the polar coordinates over a unit circle.

The step size between two adjacent blocks is equal to 2 pixels to decrease the numbers of overlapping circular blocks for reducing computational complexity. In the colour image (I) of size (M × N) in this step, we obtain $(M - 2r + 1) \times (N - 2r + 1)$ circular blocks, where r is the radius of the block and is empirically determined as equal to 7.5.

3.2 Feature Extraction

In CMFD, feature extraction is used to compute the important value or characteristic of each block (or segment or key point). An excellent feature descriptor or extraction must be able to extract high discriminative feature and robust to geometric attacks (e.g. scale and rotation) and photometric attacks (e.g. blurring, additive noise and JPG compression). Thus, QPCET

in polar coordinates is adopted in this study to extract features of circular blocks. As obtained in [28], QPCET in polar coordinates provides supreme results compared with other current methods in terms of robustness against noise and rotation, precision, numerical constancy and CPU cycle speed. As demonstrated in [29], moments in the polar regions can be calculated using QPCET. We use the same approach as in [30, 31] to replace the pixels from traditional square to circular form.

For any colour image f (x, y), the right-hand side of quaternion moments (QPCET) are precisely calculated in polar coordinates as follows [29]:

$$M_{LT}^{P} = \frac{1}{\pi}\sum_{a}\sum_{b}\hat{f}(r_a,\theta_{a,b})\, I_L(r_a) I_T(\theta_{a,b}) \qquad (1)$$

with

$$I_L(r_a) = \int_{Y_a}^{Y_{a+1}} P_L(r) r dr \qquad (2)$$

$$I_T(r_a) = \int_{X_a,b}^{X_{a,b+1}} e^{-\mu T\theta} d\theta \qquad (3)$$

where μ indicates a unit pure quaternion that is calculated as $\mu = (i+j+K)/\sqrt{3}$. $\theta_{ij} = tan^{-1}(\frac{y_i}{x_i})$, and the interpolated function of colour image is indicated by $\hat{f}(r_a,\theta_{a,b})$. Using RGB components and quaternion algebra, this function can be rewritten as follows:

$$\hat{f}(r_a,\theta_{a,b}) = \hat{f}_R(r_a,\theta_{a,b})a + \hat{f}_G(r_a,\theta_{a,b})b + \hat{f}_B(r_a,\theta_{a,b})k, \quad (4)$$

where $\hat{f}(r_a,\theta_{a,b}), \hat{f}_R(r_a,\theta_{a,b}), \hat{f}_G(r_a,\theta_{a,b})\ and\ \hat{f}_B(r_a,\theta_{a,b})$ represent the interpolated image functions deduced from the original colour image by cubic interpolation method. Here, $(r_a,\theta_{a,b})$ represents image pixel coordinate in polar form, which corresponds to the Cartesian coordinate (x, y). a, b and k denote complex operators calculated from quaternion representation following [32]. The QPCET moments in Equation (1) is obtained depending on quaternion algebra using the RGB colour channels as follows [29]:

$$M_{LT}^{P} = A_{LT}^{P} + aB_{LT}^{P} + bC_{LT}^{P} + kD_{LT}^{P}, \qquad (5)$$

where

$$A_{LT}^{P} = -\frac{1}{\sqrt{3}}\{imag[M_{LT}(\hat{f}_R)] + imag[M_{LT}(\hat{f}_G)] + imag[M_{LT}(\hat{f}_B)]\}$$
$$B_{LT}^{P} = real[M_{LT}(\hat{f}_R)] + \frac{1}{\sqrt{3}}\{imag[M_{LT}(\hat{f}_G)] - imag[M_{LT}(\hat{f}_B)]\}$$
$$C_{LT}^{P} = real[M_{LT}(\hat{f}_G)] + \frac{1}{\sqrt{3}}\{imag[M_{LT}(\hat{f}_B)] - imag[M_{LT}(\hat{f}_R)]\}$$
$$D_{LT}^{P} = real[M_{LT}(\hat{f}_B)] + \frac{1}{\sqrt{3}}\{imag[M_{LT}(\hat{f}_R)] - imag[M_{LT}(\hat{f}_G)]\} \qquad (6)$$

where conventional PCETs for the red, green and blue channels are represented by $M_{LT}(\hat{f}_R), M_{LT}(\hat{f}_G)$ and $M_{LT}(\hat{f}_B)$, respectively. a, b and k are calculated following [32]. Equation (6) exhibits the calculation of QPCET moments based on reckoning of the traditional PCET moments for the three-channel images. Consequently, the highly precise calculation of PCET moments produces highly accurate QPCR moments. Similar to [9, 29], Equations 2 and 3 can be written as the lower and upper limits of the definite integrals to deal with colour images as follows:

$$Y_{i+1} = P_a + \Delta P_a/2 \quad , \quad Y_a = P_a - \Delta P_a/2 \tag{7}$$

$$X_{a,b+1} = \theta_{a,b} + \Delta\theta_{a,b}/2 \quad , \; X_{a,b} = \theta_{a,b} - \Delta\theta_{a,b}/2 \tag{8}$$

When the rules of quaternion algebra and definite integrals are applied, the following condition is obtained.

$$I_L(r_a) = \left(\frac{e^{-\mu 2\pi L Y_{a,b}^2} - e^{-\mu 2\pi L Y_a^2}}{-\mu 4\pi L}\right) \tag{9}$$

For $L \geq 1 \; with$

$$I_0(r_a) = \left(\frac{Y_{a+1}^2 - Y_a^2}{2}\right) \tag{10}$$

and

$$I_T(\theta_{a,b}) = \begin{cases} \frac{\mu}{T}(e^{-\mu T X_{a,b+1}} - e^{-\mu T X_{a,b}}), & T \neq 0 \\ X_{a,b+1} - X_{a,b}, & T = 0 \end{cases} \tag{11}$$

Equation (11) is written depending on the rule Euler formula shown as follows [32]:

$$\frac{\mu}{T}(e^{-\mu T X_{a,b+1}} - e^{-\mu T X_{a,b}}) = \frac{\mu}{T}\{[cos(TX_{a,b+1}) - \mu \, sin(TX_{a,b+1})] - [cos(TX_{a,b}) - \mu \, sin\,(TX_{a,b})]\} \tag{12}$$

The terms of Equation 12 are reordered through [29]

$$\frac{\mu}{T}(e^{-\mu T X_{a,b+1}} - e^{-\mu T X_{a,b}}) = \frac{\mu}{T}\{C_1 - \mu C_2\} \tag{13}$$

with

$$C_1 = [cos(TX_{a.b+1}) - cos(TX_{a,b})] \tag{14}$$

$$C_1 = [sin(TX_{a.b+1}) - sin(TX_{a,b})] \tag{15}$$

Equations (14) and (15) are simplified depending on the theorems of trigonometric functions as follows [29]:

$$C_1 = -2\ sin\left[\frac{T}{2}\left(X_{a,b+1} - X_{a,b}\right)\right] \sin\left[\frac{T}{2}\left(X_{a,b+1} - X_{a,b}\right)\right] \quad (16)$$

$$C_2 = -2\ cos\ \left[\frac{T}{2}\left(X_{a,b+1} - X_{a,b}\right)\right] \sin\left[\frac{T}{2}\left(X_{a,b+1} - X_{a,b}\right)\right] \quad (17)$$

When Equations (16) and (17) utilise Equation (8), the following condition is obtained.

$$C_1 = -2sin\left(T\theta_{a,b}\right)\ sin\left[\frac{T}{2}\Delta\theta_{a,b}\right] \quad (18)$$

$$C_2 = -2cos\left(T\theta_{a,b}\right)\ sin\left[\frac{T}{2}\Delta\theta_{a,b}\right] \quad (19)$$

When we substitute $\theta_{a,b}$ and $\Delta\theta_{a,b}$ in Equations (18) and (19), we obtain

$$C_1 = -2sin\left[T\frac{\pi(2a+1)}{(8a+4)}\right] \sin\left[T\frac{\pi}{(8a)+4}\right] \quad (20)$$

$$C_2 = 2cos\left[T\frac{\pi(2b+1)}{(8a+4)}\right] \sin\left[T\frac{\pi}{(8a)+4}\right] \quad (21)$$

In the same context, when Equations (20) and (21) are substituted in Equations (9) and (10), we obtain [29]

$$I_T\left(\theta_{a,b}\right) = \begin{Bmatrix} \frac{\mu}{T}\{C_1 - \mu C_2\} & T \neq 0 \\ \Delta\theta_{a,b} & T = 0 \end{Bmatrix} \quad (22)$$

On the basis of the basics of exponent function, we write

$$\left(e^{-\mu 2\pi L Y_{a+1}^2} - e^{-\mu 2\pi L Y_a^2}\right) = \left[cos(2\pi L Y_{a+1}^2) - cos(2\pi L Y_a^2)\right] - \mu\left[sin(2\pi L Y_{a+1}^2) - sin(2\pi L Y_a^2)\right] \quad (23)$$

Using the same simplification above, Equation (9) can be rewritten as follows:

$$I_L(\theta_a) = \frac{(V_1 - \mu V_2)}{-\mu 4\pi L}, \quad (24)$$

where V1 and V2 can be represented by [9, 32]

$$V_1 = -2sin\left[L\pi\left(\frac{8a^2 + K_a}{N^2}\right)\right] \sin\left[L\pi\left(\frac{K_a}{N^2}\right)\right] \quad (25)$$

$$V_2 = -2cos\left[L\pi\left(\frac{8a^2 + K_a}{N^2}\right)\right] \sin\left[L\pi\left(\frac{K_a}{N^2}\right)\right] \quad (26)$$

We reconstruct the original colour image depending on the inverse QPCETs with a finite number of QPCET moments with the following form [29]:

$$\hat{f}(r,\theta) = \widehat{f_A}(r,\theta) + \widehat{f_B}(r,\theta)a + \widehat{f_C}(r,\theta)b + \widehat{f_D}(r,\theta)K, \quad (27)$$

where

$$\begin{aligned}
\hat{f}(r,\theta) &= \widehat{f_A}(r,\theta) + \widehat{f_B}(r,\theta)a + \widehat{f_C}(r,\theta)b + \widehat{f_D}(r,\theta)K \\
\widehat{f_A}(r,\theta) &= real\left(\acute{A}_{LT}^{P}\right) - \frac{1}{\sqrt{3}}\left[imag\left(\acute{B}_{LT}^{P}\right) + imag\left(\acute{C}_{LT}^{P}\right) + imag\left(\acute{D}_{LT}^{P}\right)\right] \\
\widehat{f_B}(r,\theta) &= real\left(\acute{B}_{LT}^{P}\right) + \frac{1}{\sqrt{3}}\left[imag\left(\acute{A}_{LT}^{P}\right) + imag\left(\acute{C}_{LT}^{P}\right) - imag\left(\acute{D}_{LT}^{P}\right)\right] \\
\widehat{f_C}(r,\theta) &= real\left(\acute{C}_{LT}^{P}\right) + \frac{1}{\sqrt{3}}\left[imag\left(\acute{A}_{LT}^{P}\right) - imag\left(\acute{B}_{LT}^{P}\right) + imag\left(\acute{D}_{LT}^{P}\right)\right] \\
\widehat{f_D}(r,\theta) &= real\left(\acute{D}_{LT}^{P}\right) + \frac{1}{\sqrt{3}}\left[imag\left(\acute{A}_{LT}^{P}\right) + imag\left(\acute{B}_{LT}^{P}\right) - imag\left(\acute{C}_{LT}^{P}\right)\right] \quad (28)
\end{aligned}$$

The value of $\widehat{f_A}(r,\theta)$ is exceedingly approaching 0. The three channels of the re-established colour image are indicated by $\widehat{f_B}(r,\theta), \widehat{f_C}(r,\theta)$ *and* $\widehat{f_D}(r,\theta)$. The reconstruction matrix of A_{LT}^{P}, B_{LT}^{P}, C_{LT}^{P} and D_{LT}^{P} can be described by $\acute{A}_{LT}^{P}, \acute{B}_{LT}^{p}, \acute{C}_{LT}^{P}$ and $\acute{D}_{LT}^{P}$, respectively [29].

$$\begin{aligned}
\acute{A}_{LT}^{P} &= \sum_{L=-\infty}^{\infty}\sum_{T=-\infty}^{\infty} A_{LT}^{P} e^{\mu\pi Lr^2 i} e^{\mu T\theta} \approx \sum_{L=-Lmax}^{L\,max}\sum_{T=-Tmax}^{T\,max} A_{LT}^{P} e^{\mu\pi Lr^2} e^{\mu T\theta} \\
\acute{B}_{LT}^{P} &= \sum_{L=-\infty}^{\infty}\sum_{T=-\infty}^{\infty} B_{LT}^{P} e^{\mu\pi Lr^2 i} e^{\mu T\theta} \approx \sum_{L=-Lmax}^{L\,max}\sum_{T=-Tmax}^{T\,max} B_{LT}^{P} e^{-\mu\pi Lr^2} e^{\mu T\theta} \\
\acute{C}_{LT}^{P} &= \sum_{L=-\infty}^{\infty}\sum_{T=-\infty}^{\infty} C_{LT}^{P} e^{\mu\pi Lr^2 i} e^{\mu T\theta} \approx \sum_{L=-Lmax}^{L\,max}\sum_{T=-Tmax}^{T\,max} C_{LT}^{P} e^{-\mu\pi Lr^2} e^{\mu T\theta} \\
\acute{D}_{LT}^{P} &= \sum_{L=-\infty}^{\infty}\sum_{T=-\infty}^{\infty} D_{LT}^{P} e^{\mu\pi Lr^2 i} e^{\mu T\theta} \approx \sum_{L=-Lmax}^{L\,max}\sum_{T=-Tmax}^{T\,max} D_{LT}^{P} e^{-\mu\pi Lr^2} e^{\mu T\theta} \quad (29)
\end{aligned}$$

We also obtain three feature vectors for each circular block (one for each of colour channel red, green and blue). These feature vectors are placed in separate matrices (FM1, FM2 and FM3, where the vector becomes a row of the respective matrix) to implement the subsequent block matching. This separation of QPCET operators to three feature vector matrices reduces feature vector size and simultaneously improves detection accuracy.

3.3 Block Matching

After generating the feature vectors of a block, potential copy–move pairs are identified by searching blocks with similar feature vectors. In most CMFD algorithms, lexicographic sorting is used. This usage is sensitive to transformations and produces reliable results with lower false negative rates than KD-tree [33]. The duplication region is identified using the KD-tree [34] algorithm for block matching. The KD-tree is a commonly used structure for searching the nearest neighbour (NN). Feature matching is performed through KD-tree-based

methods (FLANN package) similar to [34, 35]. FLANN is a popular library for performing rapid approximate NN search. NN is selected using the minimum Euclidean distance between two feature vector elements. The distance between two block features in terms of Euclidean distance metric is expressed as

$$d\left(\overrightarrow{F1},\overrightarrow{F2}\right)=\sqrt{\sum_{i=1}^{p}(F1_i-F2_i)^2}, \qquad (30)$$

where P is the dimension of the feature vector, and $\mathbf{F1_i}$ and $\mathbf{F2_i}$ are the i^{th} row of the block. The forged regions are correctly detected by tallying the distances of the closest neighbour blocks with the pre-determined similarity threshold T_ (Similar). For (d < T)-(Similar), two blocks of image are similar. Otherwise, the pairs are dissimilar and are deleted from the potential similarity group.

The potential block matching is an unnecessary forged area because most natural images contain many contiguous areas with similar intensities (e.g. sky), and this condition causes false matching. The Euclidean distance between two corresponding blocks is calculated to filter out weak matches for reducing the probability of false matching. f (x_i , y_i) and (x_j , y_j) are the coordinates of the centre pixel in the two-potential pair. The Euclidean distance is calculated by

$$\boldsymbol{Distance}(\boldsymbol{B_1},\boldsymbol{B_2})=\sqrt{\left(\boldsymbol{x_i}-\boldsymbol{x_j}\right)^2+\left(\boldsymbol{y_i}-\boldsymbol{y_j}\right)^2}. \qquad (31)$$

If the distance of two overlapping blocks is more than the predefined distance threshold, then the distance of the two blocks is considered forgery. Otherwise, they are close and must be removed. If this pair possesses more than six neighbouring pairs, then the neighbourhoods of the two blocks are likely to be similar for further verification. Thus, all possible matches are collected and arranged in an array called matrix matching or corresponding matrix (CM). The number of rows in the matrix is called the block number, and two columns consist the block index (representing the centre of block) of the corresponding block pairs. Similarly, for feature matrices FM2 and FM3, we obtain CM2 and CM3. A block is matched with another block in each of corresponding matrices, CM1, CM2 and CM3. The candidate copy–moved blocks are determined using the majority rule. For each block, if at least two corresponding matrices show the same results, then those blocks are considered real copy–moved blocks.

3.4 Post-processing of Detection Result

During block matching, some false matching may occur for non-duplicated regions with similar features. In general, some falsely detected blocks are marked on the initial detection due to homogeneity in image content. The textures of these blocks have similarities, and this undesirable effect is noticeable in smooth regions. Thus, the results obtained via block matching step are not precise and require major refinement. An improved RANSAC algorithm is implemented to overcome the limitations of RANSAC [36]. Moreover, RANSAC algorithm is used to identify inliers between matching blocks in the SBM data points that are related via rotation, scaling and translation [37]. Thus, the other false matches (outliers) are removed. The affine transform matrix of the copied region and the pasted

region is computed by the points randomly chosen from the matched points set by the following formula:

$$\begin{bmatrix} u \\ v \end{bmatrix} = \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} t_x \\ t_y \end{bmatrix}, \quad (32)$$

where (x, y) and (u, v) represent the corresponding matched block. $m1$, m_2, m_3, m_4, t_x and t_y are the six parameters of the affine transform.

A model is estimated by the least square method, and the matched block set is divided into two groups of points including inliers and outliers. Unlike traditional RANSAC (in which inlier points are included, whereas outlier points are excluded), inliers are saved as the match points. The RANSAC is re-implemented on the potential corresponding points (outlier points are rejected from the first execution of RANSAC). Six iterations of RANSAC are executed (number of iterations is related to the number of repetitive regions to be disclosed). All inliers are saved as the final detection. The detected region boundaries are smoothened, and tiny holes in the map are filled. Morphological erosion is conducted to remove the large regions and ensure that the detected regions retain the original size when the morphological dilation is performed. **Fig. 2** shows the detection results of the method after performing the proposed post-processing steps.

Fig. 2. Copy–move forgery detection result: (left) tampered image, (middle) initial result on detection with false positive and (right) result after false positive removal.

4. Results and Discussion

In this section, a series of experiments is conducted to evaluate the excellent robustness and high efficiency of the presented CMFD method using different metrics in which the forged regions are variously manipulated. All experiments are performed using MATLAB version 2017a and computed using a personal computer (2.1 GHz CPU with 4 GB memory).

The implementation of the proposed method is evaluated using images from the CMFD database, which was built by Tralic et al. [38]. All these images are recorded by a Canon EOS 7D camera and stored in the CR2 (Canon RAW version 2) format as minimally processed data. All images are coloured with 512 × 512 pixel size and PNG format. Following Tralic et al. [38], the images in the CMFD database are divided into different groups depending on the type of manipulation applied. These groups include numbers of images that vary from one group to another as follows: 40 images for each of simple CMF, rotation and scaling; 120 images for each of blurring, brightness, colour reduction and adaptive Gaussian Noise dataset; and 320 images for the JPEG compression group of the

CMFD database. In addition to previous manipulation, this database includes combination attacks, which are ignored in this study. Every image possesses its own binary reference map (ground truth) for validation. The approximate dimension of counterfeit regions in all forged images in the CoMoFoD dataset differs between 24 × 15 pixels to 174 × 174 pixels. The performance of the proposed CMFD method is measured in terms of correct detection ratio (CDR) and false detection ratio (FDR), which are defined as

$$\mathrm{CDR} = \frac{\left|\mathrm{C} \cap \tilde{C}\right| + \left|\mathrm{F} \cap \tilde{F}\right|}{|\mathrm{C}| + |\mathrm{F}|}, \qquad (33)$$

$$\mathrm{FDR} = \frac{|\tilde{C} - \mathrm{C}| + |\tilde{F} - \mathrm{F}|}{|\tilde{C}| + |\tilde{F}|}, \qquad (34)$$

where C is the copied region; F is the tampered one; $\tilde{\mathrm{C}}$ is the detected copy region; $\tilde{\mathrm{F}}$ is the detected tampered region; modulus (| |) refers to the area of the region; and ∩ denotes the intersection of two regions. CDR reflects the performance of the algorithm in correctly locating the pixels of copy–move regions in the tampered image, and FDR measures the percentage of pixels outside the duplicated region but are included by the implemented method. The method is precise if CDR is close to 1 and FDR is close to 0.

The effectiveness and robustness of the proposed CMFD approach is assessed using a series of separate experiments. These experiments are classified into absence and presence of post-processing, and attack types include simple CMF, photometric attack (i.e. blurring, brightness, colour reduction and adaptive Gaussian noise and JPEG compression) and geometric attack (rotation and scaling). The results are compared against those of state-of-the-art techniques and discussed at end of this section. Notably, the measures CDR and FDR in the subsequent practical tests refer to the calculated average value for set of images in each experiment.

In the first experiment, we test the detection performance under ideal conditions (without post-processing). In this type of image, the forged region is simply copied, moved and pasted to a new location within the same image without applying any distortion-assisted processing. Experiments are performed by selecting the first 40 images from the CoMoFoD database. Following Tralic et al. [38], the first 40 images (with numbers 001 to 040) are used for simple CMF and are not exposed to any type of photometric, rotation and scale attacks. **Fig. 3** illustrates the excellent detection capacity of the present method even when the tampered image has multiple copied regions. The CDR of the proposed method is approximately 0.998, whereas the FDR is around 0.002 after applying post-processing.

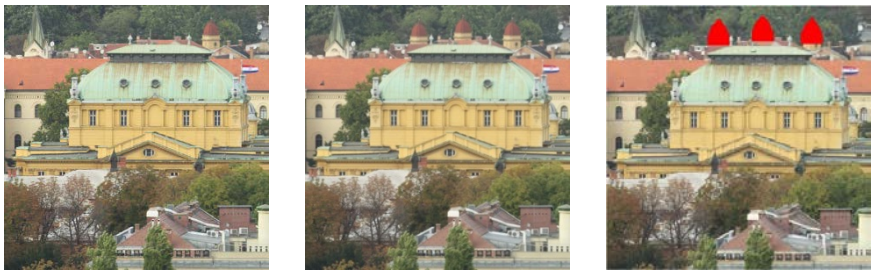


Fig. 3. Forgery detection in images with multiple copy–move tampering: (left) original image, (middle) tampered image and (right) detection result.

As mentioned previously, the capacity to resist photometric attacks is a major concern in CMFD. Several photometric attacks such as blurring, brightness, colour reduction, JPEG compression and additive noise can be used to hide traces of tampering and produce seamlessly integrated images that make the forgery detection greatly intricate. Thus, the second set of experiments is devoted to test the effectiveness of the proposed detection method in case of counterfeit images exposed to this type of attack.

The capability of the proposed algorithm to resist blurring attacks is evaluated on 120 forged images from the CoMoFoD database. These images are created by convolving each image using three different averaging filters as masks, namely, (3 × 3), (5 × 5) and (7 × 7). Images blurred by any of the averaging filters are noticeably altered, particularly for 7 × 7 averaging filters. The results are depicted in **Fig. 4** (first row). **Table 1** lists the statistical detection rates of blurring duplication utilising various averaging filters. Detection performance is superior when the distortion is made using (3 × 3) and (5 × 5) averaging filters. However, the detection results are inferior when (7 × 7) averaging filter is utilised. Therefore, the statistical detection rate of blurring attack-assisted images is similar to that of translation duplication, especially with (3 × 3) averaging filters.

Table 1. Evaluation results on robustness against blurring attacks.

Image Blurring (Filter size)	**3 × 3**	**5 × 5**	**7 × 7**	**Average**
CDR	0.996	0.980	0.965	0.980
FDR	0.002	0.011	0.056	0.023

The robustness of the developed technique against brightness adjustment attacks are evaluated using 120 images forged with brightness alteration. This change is performed by limiting the original image intensity within lower and upper bound intervals of [0, 1]. Accordingly, three ranges of brightness, namely, [0.01, 0.95], [0.01, 0.9] and [0.01, 0.8], are obtained from the CoMoFoD database (only these ranges of brightness are found in this database) [38]. The image brightness altered by [0.01, 0.95] is imperceptible, and a change of [0.01, 0.8] is visually different in the post-processed image. **Fig. 4** (second row) illustrates the visual detection results for tampered images in which the brightness is altered by [0.01, 0.8]. **Table 2** summarises the statistical detection rates under various brightness conditions. The detection performance of the proposed method remains reliable even in the range of [0.01, 0.8]. This result confirms the excellent robustness of the algorithm against image brightness changes.

Table 2. Evaluation results on robustness against brightness change attacks.

Brightness Adjustment (lower and upper bound)	[0.01, 0.95]	[0.01, 0.9]	[0.01, 0.8]	Average
CDR	0.997	0.994	0.985	0.992
FDR	0.005	0.007	0.031	0.014

Robustness against colour reduction attacks is tested. Images are selected from the same dataset (CoMoFoD database). Colour reduction conducted using uniform quantisation of intensity values. Each colour channel in the forged image, the number of intensity level decreased from 256 (original image) to 128, 64 and 32. Images obtained by decreasing intensity levels have nearly imperceptible degradation compared with original one. **Fig. 4** (third row) shows a tampered image with colour reduction and its corresponding detection result. **Table 3** lists the detection results for a tampered image that is distorted by colour reduction. The proposed method performs excellently for colours with high bit depth (128), which is due to the low-density reduction at high depth level. Furthermore, this method achieves high rates even with low levels (32 and 64) of colour reduction attacks.

Table 3. Evaluation results on robustness against colour reduction attacks.

Colour Reduction (Levels)	32	64	128	Average
CDR	0.985	0.988	0.9943	0.989
FDR	0.040	0.025	0.017	0.27

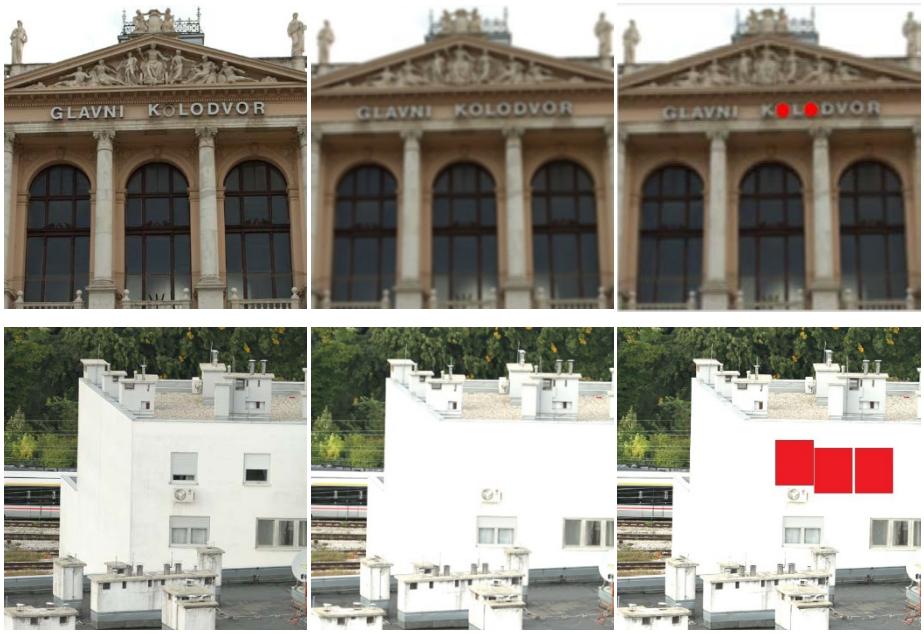


Fig. 4. Forgery detection in images with multiple copy–move tampering: (left) original image, (middle) tampered image and (right) detection result. The first, second and third rows represent blurring, brightness and colour reduction attacks, respectively.

The robustness of the proposed CMFD against JPEG compression attack is also determined. In this experiment, images are distorted by varying the quality factor between 20 and 100 in 10 steps. The same CoMoFoD dataset is also used to determine the performance of the method. **Table 4** lists the performance superiority of the proposed method regardless of the quality factor variation during compression. The CDR exceeds 0.9 even if the forged images are compressed with a quality factor of 60. In most cases, the constant value of FDRs (below 0.1) indicates the excellent performance of the proposed algorithm. This method can detect JPEG compression with a quality factor above 40, which results in acceptable CDR and FDR values.

Table 4. Evaluation results on robustness against JPEG compression attacks.

Quality Factor	90	80	70	60	50	40	30	20	Average
CDR	0.982	0.966	0.935	0.915	0.856	0.872	0.745	0.66	0.866
FDR	0.029	0.061	0.071	0.11	0.132	0.176	0.381	0.52	0.185

The last experiment in this set evaluates the robustness of the proposed scheme against Gaussian noise attacks. In this experiment, 120 images are selected from the CoMoFoD database, and Gaussian white noise with zero mean and three different variances (0.009, 0.005, 0.0005) are incorporated within each image. **Table 5** summarises the overall accuracy of the proposed CMFD scheme under Gaussian noise.

Table 5. Evaluation results on robustness against Gaussian noise attacks.

Additive Noise (Variance)	0.009	0.005	0.0005	Average
CDR	0.89	0.93	0.96	0.926
FDR	0.15	0.11	0.056	0.105

In addition to the previously mentioned attacks, the tampered images may be exposed to geometric attacks such as rotation and scaling that make detection difficult. Therefore, the third set of experiments is focused on assessing the robustness of the proposed CMFD in the presence of rotation and scaling attacks. For the rotation attack, each image used includes

one or two forged regions by rotation with varying rotational angles (between 1° and 180°). In case of the scaling attack, the forged region is copied and resized via scaling up or down using a scaling factor from 0.4 to 1.5. Excerpts of the experimental results in case of the presence of the rotation and scaling attacks are illustrated in **Figs.** 5 **and** 6, respectively. **Tables 6 and 7** list the statistical detection rates obtained by the proposed CMFD in the presence of the same attacks. The results reveal that the proposed CMFD achieves high accuracy with CDRs of nearly 0.921 and 0.909 on average for rotation and scaling attacks, respectively.

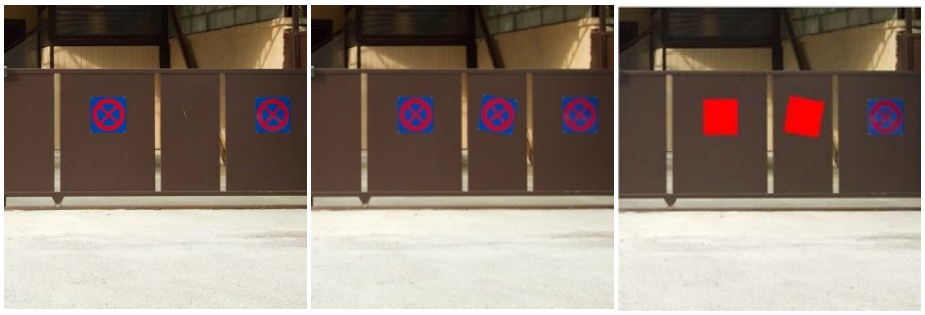


Fig. 5. Detection results using images under distortion by rotation: (left) original image, (middle) tampered image with rotated forged region by 10° and (right) final detection.

Table 6. Robustness against rotation attacks.

Rotation Angles	**2**	**4**	**6**	**8**	**10**	**20**	**60**	**90**	**180**	**Average**
CDR	0.98	0.96	0.953	0.92	0.9	0.89	0.88	0.90	0.91	0.921
FDR	0.09	0.12	0.143	0.172	0.200	0.23	0.256	0.295	0.300	0.20

Fig. 6. Detection results using images under distortion by scaling: (left) original image, (middle) tapered image after scaling the duplicated region with a scale factor of 1.03 and (right) final detection.

Table 7. Robustness against scale invariance.

Scale factor	0.90–0.94	0.95–0.99	1.01–1.05	1.06–1.10	average
CDR	0.875	0.923	0.945	0.896	0.909
FDR	0.145	0.045	0.123	0.067	0.095

The detection performance of the proposed CMFD is compared with that of the state-of-the-art techniques in literature that used the same CoMoFoD dataset and validation metrics to achieve fair comparison. **Table 8** presents a comparison of the proposed approach with other popular approaches, namely, HOG [3], HOGM [39], PCET [40], LGWP [41] and Convolutional Kernel Network [42]. The proposed CMFD based on QPCET descriptors provide superior detection efficiency to previous methods. Therefore, the performance of any forgery detection scheme with block matching method fundamentally depends on the invariant features used to extract block features and the method used to find the similar block features.

Table 8. Performance comparison of the proposed method with other existing techniques.

			Type of Attack						
Author(s)/ Year	**Features Extraction**	**Quality Factor**	**Blurring Attacks**	**Brightness**	**Colour Reduction**	**Compression**	**Adaptive Noise**	**Rotation**	**Scaling**
Lee, Chang, & Chen,[3]	HOG	CDR	0.972	0.990	0.986	n/a	n/a	0.864	n/o
		FDR	0.036	0.018	0.035			0.286	
Lee [39]	HOGM	CDR	0.968	0.971	n/a	0.76	n/a	0.55	0.71
		FDR	0.051	0.034		0.22		0.55	0.34
Emam, Han, & Niu [40]	PCET	CDR	0.893	0.921	n/a	0.812	0.825	0.871	0.83
		FDR	0.035	0.193		0.232	0.187	0.312	0.193
Chou & Lee [41]	LGWP	CDR	0.961	0.973	n/a	0.714	n/a	0.501	n/a
		FDR	n/a	n/a		n/a		n/a	
Liu, Guan, & Zhao [42]	Convolutional Kernel Network	CDR	0.827	0.784	0.844	0.726	0.781	0.900	0.751
		FDR	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Proposed Method	QPCET	CDR	0.980	0.992	0.989	0.866	0.926	0.921	0.909
		FDR	0.023	0.014	0.27	0.185	0.105	0.20	0.095

The overall test results indicate that our proposed approach can obtain effective detection results for CMF of colour images under various challenging conditions. The results for simple CMF reveal that the performance of the proposed method is nearly complete and flawless with a nearly perfect CDR and an FDR that is decreased to nil in all categories. The results for photometric attacks shown in **Tables 1 to 5** indicate that the method achieves encouraging performance with a CDR in between 0.866 and 0.992. The results for geometric attacks also reveal that the proposed CMFD achieves high accuracy with a CDR of nearly [0.980 and 0.88] on average for rotation but a CDR between [0.945 and 0.875] for scaling attacks. The lowest CDRs are 0.88 and 0.875 for rotation and scaling, respectively. Nevertheless, the proposed CMFD locates the forged region without failing. The imperfection is due to some missing pixels during post-processing stage for removing false positives. This study can reaffirm that the proposed CMFD is robust against geometric attacks. The proposed method is also compared with other existing methods that used the same CoMoFoD dataset to demonstrate the robustness of the method. **Table 8** shows that the achieved results not only are promising but also are the best in this dataset. Despite the

encouraging results of the proposed system, it still requires considerable processing time with an average processing time of processing 455 s. Therefore, the efficiency of block-based forgery detection fundamentally depends on the method used to extract robust feature and the method used in matching and post-processing.

5. Conclusion

CMFD has become inevitable with the ever-increasing growth of digital multimedia for information exchange across networks. An efficient forensic method for CMFD is proposed in digital images based on the QPCET for invariant colour image description. Experiments are also performed by developing the MATLAB algorithm with the inclusion of various tampering (geometric and photometric) on images acquired from the CoMoFoD dataset. The results of the proposed method are evaluated and compared with those of existing state-of-the-art techniques. The proposed algorithm is demonstrated to be accurate and efficient in detecting multiple CMF instances. The method is also robust against actions aimed at concealing forgeries including geometric (e.g. rotation and scaling) and photometric attacks (e.g. blurring, brightness, colour reduction, compression, adaptive noise and JPEG compression). The results for all cases are very encouraging with a CDR of 0.998 achieved for normal tampered images but a CDR between 0.866 and 0. 992 for the ones with photometric attacks. For images under rotation and scaling attacks, the average CDR is between 0.921 and 0.909. The proposed CMFD markedly outperforms existing methods based on HOG, HOGM and PCET. The present algorithm reveals weak detection performance on duplicated images with affine transformation and is time consuming despite the QPCET has CPU cycle speed. Admirable features of the proposed method suggest that it may valuably contribute toward the development of multimedia forensics. The forthcoming plan includes making the method robust against challenging tampering conditions (e.g. affine transformations and combination attacks) and accelerating its running time.

Acknowledgment

The author would like to thank Mustansiriyah University (www.uomustansiriyah.edu.iq) Baghdad-Iraq for its support in the present work.

References

[1] Redi, J.A., W. Taktak, and J.-L. Dugelay, “Digital image forensics: a booklet for beginners,” *Multimedia Tools and Applications*, vol. 51, no. 1, pp. 133-162, 2011. Article (CrossRef Link).

[2] Mahdian, B. and S. Saic, “A bibliography on blind methods for identifying image forgery,” *Signal Processing: Image Communication*, vol. 25, no. 6, pp. 389-399, 2010. Article (CrossRef Link).

[3] Lee, J.-C., C.-P. Chang, and W.-K. Chen, “Detection of copy–move image forgery using histogram of orientated gradients,” *Information Sciences*, vol. 321, pp. 250-262, 2015. Article (CrossRef Link).

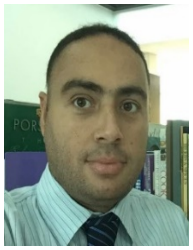
[4] Sridevi, M., C. Mala, and S. Sanyam, “Comparative study of image forgery and copy-move techniques,” *Advances in Computer Science, Engineering & Applications*, pp. 715-723, 2012. Article (CrossRef Link).

[5] Tralic, D., et al., “Copy-move forgery detection using cellular automata, in Cellular Automata in Image Processing and Geometry,” *Cellular Automata in Image Processing and Geometry*, pp. 105-125, 2014. Article (CrossRef Link).

[6] Elwin, J.G.R., T. Aditya, and S.M. Shankar. "Survey on passive methods of image tampering detection," in *Proc. of IEEE Conf. on Communication and computational intelligence*, 2010. Article (CrossRef Link).
[7] Shih, F.Y. and Y. Yuan, "16 A Comparison Study on Copy–Cover Image Forgery Detection," *Multimedia Security: Watermarking, Steganography, and Forensics*, pp. 297, 2012.
[8] Ryu, S.-J., et al., "Rotation invariant localization of duplicated image regions based on Zernike moments," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 8, pp. 1355-1370, 2013. Article (CrossRef Link).
[9] Wang, X.-y., et al., "Quaternion polar complex exponential transform for invariant color image description," *Applied Mathematics and Computation*, vol. 256, pp. 951-967, 2015. Article (CrossRef Link).
[10] Sheng, Y., H. Wang, and G. Zhang, "Comparison and Analysis of Copy-Move Forgery Detection Algorithms for Electronic Image Processing," *Advances in Mechanical and Electronic Engineering*, pp. 343-348, 2013. Article (CrossRef Link).
[11] Fridrich, A.J., B.D. Soukal, and A.J. Lukáš, "Detection of copy-move forgery in digital images," in *Proc. of Digital Forensic Research Workshop, Citeseer*, 2003. Article (CrossRef Link).
[12] Popescu, A. and H. Farid, "Exposing digital forgeries by detecting duplicated image region [Technical Report]," *Hanover, Department of Computer Science, Dartmouth College. USA*, pp. 32, 2004.
[13] Wandji, N.D., S. Xingming, and M.F. Kue, "Detection of copy-move forgery in digital images based on DCT," *arXiv preprint arXiv:1308.5661*, 2013. Article (CrossRef Link).
[14] Ghorbani, M., M. Firouzmand, and A. Faraahi, "DWT-DCT (QCD) based copy-move image forgery detection," in *Proc. of IEEE Conf. on Systems, Signals and Image Processing*, 2011. Article (CrossRef Link).
[15] Sunil, K., D. Jagan, and M. Shaktidev, "DCT-PCA based method for copy-move forgery detection," in *Proc. of 48th Annual Convention of Computer Society of India Conf. on ICT and Critical Infrastructure, Springer*, pp. 577-583, 2014. Article (CrossRef Link).
[16] Mahdian, B. and S. Saic, "Detection of copy–move forgery using a method based on blur moment invariants," *Forensic science international*, vol. 171, no. 2, pp. 180-189, 2007.
[17] Li, L., et al., "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. 46-56, 2013. Article (CrossRef Link).
[18] Li, L., et al., "Detecting copy-move forgery under affine transforms for image forensics," *Computers & Electrical Engineering*, vol. 40, no. 6, pp. 1951-1962, 2014. Article (CrossRef Link).
[19] Zhong, J., et al., "A new block-based method for copy move forgery detection under image geometric transforms," *Multimedia Tools and Applications*, vol. 76, no. 13, pp. 14887-14903, 2017. Article (CrossRef Link).
[20] Hosny, K.M., H.M. Hamza, and N.A. Lashin, "Copy-move forgery detection of duplicated objects using accurate PCET moments and morphological operators," *The Imaging Science Journal*, vol. 66, no. 6, pp. 330-345, 2017. Article (CrossRef Link).
[21] Mahmood, T., et al., "A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform," *Journal of Visual Communication and Image Representation*, vol. 53, pp. 202-214, 2018. Article (CrossRef Link).
[22] Huang, H., W. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm," in *Proc. of IEEE Workshop on Computational Intelligence and Industrial Application*, 2008. Article (CrossRef Link).
[23] Bo, X., et al., "Image copy-move forgery detection based on SURF," in *Proc. of IEEE Conf. on Multimedia information networking and security*, 2010. Article (CrossRef Link).
[24] Zhu, Y., X. Shen, and H. Chen, "Copy-move forgery detection based on scaled ORB," *Multimedia Tools and Applications*, vol. 75, no. 6, pp. 3221-3233, 2016. Article (CrossRef Link).

[25] Amerini, I., et al., "A sift-based forensic method for copy–move attack detection and transformation recovery," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1099-1110, 2011. Article (CrossRef Link).
[26] Chen, L., et al., "Region duplication detection based on Harris corner points and step sector statistics," *Journal of Visual Communication and Image Representation*, vol. 24, no. 3, pp. 244-254, 2013. Article (CrossRef Link).
[27] Yang, F., et al., "Copy-move forgery detection based on hybrid features," *Engineering Applications of Artificial Intelligence*, vol. 59, pp. 73-83, 2017. Article (CrossRef Link).
[28] Hosny, K.M. and M.M. Darwish, "A kernel-based method for fast and accurate computation of PHT in polar coordinates," *Journal of Real-Time Image Processing*, vol. 16, no. 4, pp. 1235-1247, 2019. Article (CrossRef Link).
[29] Hosny, K.M. and M.M. Darwish, "Accurate computation of quaternion polar complex exponential transform for color images in different coordinate systems," *Journal of Electronic Imaging*, vol. 26, no. 2, pp. 023021, 2017. Article (CrossRef Link).
[30] Hosny, K.M., "Accurate orthogonal circular moment invariants of gray-level images," *Journal of Computer Science*, vol. 7, no. 5, pp. 715-722, 2011. Article (CrossRef Link).
[31] Liu, C., X.-H. Huang, and M. Wang, "Fast computation of Zernike moments in polar coordinates," *IET image processing*, vol. 6, no. 7, pp. 996-1004, 2012. Article (CrossRef Link).
[32] Hosny, K.M. and M.M. Darwish, "Highly accurate and numerically stable higher order QPCET moments for color image representation," *Pattern Recognition Letters*, vol. 97, pp. 29-36, 2017. Article (CrossRef Link).
[33] Christlein, V., C. Riess, and E. Angelopoulou. "A Study on Features for the Detection of Copy-Move Forgeries," *Sicherheit*, pp. 105-116, 2010. Article (CrossRef Link).
[34] Christlein, V., et al., "An evaluation of popular copy-move forgery detection approaches," *IEEE Transactions on information forensics and security*, vol. 7, no. 6, pp. 1841-1854, 2012. Article (CrossRef Link).
[35] Muja, M. and D.G. Lowe, "Fast approximate nearest neighbors with automatic algorithm configuration," *VISAPP*, vol. 1, no. 2, pp. 331-340, 2009. Article (CrossRef Link).
[36] Raguram, R., J.-M. Frahm, and M. Pollefeys, "A comparative analysis of RANSAC techniques leading to adaptive real-time random sample consensus," in *Proc. of Computer Vision*, pp. 500-513, 2008. Article (CrossRef Link).
[37] Davarzani, R., et al., "Copy-move forgery detection using multiresolution local binary patterns," *Forensic science international*, vol. 231, pp. 61-72, 2013.
[38] Tralic, D., et al., "CoMoFoD—New database for copy-move forgery detection," in *Proc. of IEEE symposium on ELMAR international symposium*, pp. 49-54, 2013. Article (CrossRef Link).
[39] Lee, J.-C., "Copy-move image forgery detection based on Gabor magnitude," *Journal of Visual Communication and Image Representation*, vol. 31, pp. 320-334, 2015. Article (CrossRef Link).
[40] Emam, M., Q. Han, and X. Niu, "PCET based copy-move forgery detection in images under geometric transforms," *Multimedia Tools and Applications*, vol. 75, no. 18, pp. 11513-11527, 2016. Article (CrossRef Link).
[41] Chou, C.-L. and J.-C. Lee, "Copy-Move Forgery Detection Based on Local Gabor Wavelets Patterns," in *Proc. of Springer on International Conference on Security with Intelligent Computing and Big-data Services*, vol. 733, pp 47-56, 2018.
[42] Liu, Y., Q. Guan, and X. Zhao, "Copy-move forgery detection based on convolutional kernel network," *Multimedia Tools and Applications*, vol. 77, no. 14, pp. 18269-18293, 2018. Article (CrossRef Link).

Salam A. Thajeel received the BSc degree in Computer Science from Mustansiriyah University, Baghdad-Iraq, in 2000. ; His M.Sc. degree in computer science (pattern recognition) from Iraqi Commission for Computer and Informatics, Informatics Institute for Postgraduate studies, in 2003; and his Ph.D. degree in computer science (digital forensic) from University Technology Malaysia (UTM), Johor Bahru, Malaysia, in 2016. He is currently an assistant professor in the Department of Computer Science at Mustansiriyah University, Baghdad Iraq. His research interest includes digital forensic, computer vision, multimedia information security and image processing, etc.



Ali Shakir Mahmood received the B.S. (Software Engineering) degree in 2003 from AL- Rafidain University College, Iraq; His M.Sc. degree in Computer Science (Data Security) from Iraqi Commission for Computer and Informatics, Informatics Institute for Postgraduate studies, in 2006; and his Ph.D. degree in Computer Science (Data Security) from University Technology Malaysia (UTM), Johor Bahru, Malaysia, in 2016. he is currently a lecturer at Department of Computer Science, College of Education, Mustansiriyah University, Baghdad Iraq. His research interest includes data security, image processing and pattern recognition

Waleed Rasheed Humood received B.S. degree in Computer Science from Mustansiriyah University, Iraq. in 2002, the M.S. in science in Software Engineering from Informatics Institute for Post Graduate Studies- Iraqi Commission for Computers and Informatics – Iraq in 2012. he now a lecturer at Department of Computer Science, College of Education, Mustansiriyah University, Baghdad- Iraq. his research interests include image processing, software engineering.

Ghazali Bin Sulong received bachelor's degrees in Statistics (1979) from National University of Malaysia (UKM), His M.Sc. degree in computing (1982) from the Uni. College Cardiff, Wales, U.K. In 1989 he obtained a Ph.D.in Computer Science from the Uni. College Cardiff, Wales, U.K. (formerly University of Southwestern Louisiana), USA in 1986 and 1990, respectively. He is currently a Professor in the School Informatics and Applied Mathematics at University Malaysia Terengganu (UMT), Terengganu, Malaysia. His research area interest includes Image Processing and Pattern Recognition.