UTM UNIVERSITI TEKNOLOGI MALAYSIA
INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING
ISSN 2180-4370
Journal Homepage : https://ijic.utm.my/

An Improved DCT Block Based Technique for Copy-Move Forgery Detection in Medical Images

Abdulraheem Hassanat Oyiza and Mohd Aizaini Maarof
Faculty of Computing,
Universiti Teknologi Malaysia,
81310 UTM Johor Bahru, Johor, Malaysia
Email: hassanatabdulraheem@gmail.com, aizaini@utm.my

Submitted: 12/01/2018. Revised edition: 26/03/2018. Accepted: 8/05/2018. Published online: 21/05/2018

***Abstract*—Copy-Moved forgery is a common method to manipulate images. Several attempts of image forgery have been discovered and involves a region been duplicated and copied and pasted on another region of the same image in other to achieve selfish gain. Generally, there are two classification of copy-move forgery detection technique such as the block-based and key point-based. The most commonly used technique is the block based which divides image into blocks during the stage of image pre-processing before features are extracted whereas key point based technique skips the division of image into blocks and directly extracts different local feature from the image. In this paper, we review various block based and key point approach which has been proposed by various researchers. The proposed technique is based on DCT and an improvement on DCT technique is achieved in terms of dimensionality reduction using an octagonal block to reduce the number of features for matching, thereby improving detection accuracy. Based on the analysis of this work as compared to previous proposed works, since previous work represents about 79% of the quantized DCT coefficients on each image block and this proposed work represents about 85% of quantized DCT coefficients, therefore, recovery of about 6% more features using the octagonal block was observed as the improvement over the previously proposed dimensionality reduction using the circle block.**

Keywords — DCT, DWT, DyWT, SIFT, SURF, Harris Corner, Lexicographical Sort, Radix Sort

I. INTRODUCTION

Digital images are extensively used and important in many domains. They have become part of everyday life as well as part of many applications in science. There are cheap computers and easily accessible software applications for image processing which are readily available. This makes tampering digital image without any visible traces easier. In the past, several attempts of image forgery have been discovered [1]. The commonly used method for manipulating an image are erasing or concealing a section in the image, adding something new to the image Jaberi [2], Bebis [3], and misrepresenting the image data [1]. Image forgery detection has been classified into various techniques. These detection techniques are categorized based on mechanisms that extract important features from a suspected image. Generally, detection of copy move forgery is based on block based division and key point extraction. Previously, various researchers proposed varieties of improvements based on these techniques to detect forged images. The most commonly used technique is the block wise division method. This method involves splitting images into square or circular blocks, next, the feature extraction process can take place and blocks are compared to check for similarity, thereafter, if matching blocks are detected, this will determine the presence of forgery in an image. Unlike the block based division, the key point extraction technique does not require images to be divided into blocks during pre-processing, rather, only the important features are extracted from the image [3].

II. LITERATURE REVIEW

In this section, a qualitative review of copy-move image forgery detection techniques has been revisited and presented. Image forgery detection has been classified into various techniques. These detection techniques are categorized based on mechanisms that extract important features from a suspected image. Generally, detection of

copy move forgery is based on block based division and key point extraction. Previously, various researchers proposed varieties of improvements based on these techniques to detect forged images. The most commonly used technique is the block wise division method. This method involves splitting images into square or circular blocks, next, the feature extraction process can take place and blocks are compared to check for similarity, thereafter, if matching blocks are detected, this will determine the presence of forgery in an image. Unlike the block based division, the key point extraction technique does not require images to be divided into blocks during pre-processing, rather, only the important features are extracted from the image [4], [5, 6]. Therefore, the copy-move image forgery detection technique is divided into two namely, block-based division and key point-based extraction techniques. Since our study focused more on the discrete cosine transformation approach, which is one of the approaches in block-based division techniques. Hence, the review is centered on the block-based division techniques and its approaches.

A. Block Based Division

Due to its adaptability with varieties of techniques for feature extraction and its effectiveness in relation to matching forged regions, block based division is the most preferable technique used in recent proposed works. Block based feature extraction technique can be categorized based on frequency transformation, texture and intensity, moment invariant, log polar transformation, dimension reduction and multi scale auto-convolution (MSA). The conventional process for image forgery detection using the block based division technique involves certain stages, such as the pre-processing stage, extraction of relevant feature vectors from the divided blocks, feature matching of similar blocks. This first stage involves the transformation of coloured image to grayscale to reduce size of the data and expose relevant features in an image, thus, curtailing the computational complexity and enhancing the pace at which computation is carried out. This transformation was implemented in Cao, Gao [7] by using an established formula $I = 0.228R + 0.587G + 0.114B$ to successfully change suspect image to grayscale. Another category of a pre-processing activity involves the division of suspected image into blocks. Block based division can be enhanced to reduce its processing complexity and size of feature vector without tampering with its detection efficiency by placing most of the elements in the matrix within a circle block rather than a square block before extracting relevant features. In order to achieve improvement in the complexity of feature matching, Cao, Gao [7] also used circular block to represent the co-efficient matrix, its dimensionality is measured with r (radius) and amounts to an area measured with $pi \times r^2$ by firstly splitting the image into overlapping square blocks whose dimensionality is measured by a constant B and amounts to block sizes and co-efficient matrix of $B \times B$, afterwards, used the circular block to represent a better part of it, after extracting the features.

In the next stage, feature extraction mechanism is used to obtain important feature vectors from a segmented image. The types of feature extraction mechanism for block based division approach will be discussed. Afterwards, the feature matching is carried out by searching for the correlation between extracted feature vectors and two or more block pairs. The aim of matching similar block pairs is to successfully find forged regions in an image. Methods for feature matching of block based division are classified into sorting, hash, correlation, Euclidean distance, DCT coefficients and clustering. Mapping is a process whereby forged regions in an image are vividly identified, this can be achieved by colouring those regions in order to differentiate them from the un-tampered regions [5]. Basically, feature matching is done to compare the blocks against each other to determine similar blocks. Amongst all techniques for feature matching in block based division, sorting is the most widely used technique. This technique arranges the extracted features vectors in a peculiar form. Since efficiency is required to swiftly detect forged or copy-moved regions in an image, this technique is very suitable, coupled with the fact that it reduces processing cost involved in performing the searching and merging of duplicated regions in an image.

Commonly known Sub-division of sorting technique includes the Lexicographical sort, KD Tree and Radix sort. The principle employed in lexicographical sort involves alphabetical arrangement based on values of extracted features while KD-Tree inherits the properties of a tree to perform its search in the nearest neighbor [5]. Davarzani, Yaghmaie [8] proposed a method to extract feature vectors from an image by using local binary pattern (LBP), and then ordered these feature vectors using lexicographical sort technique. Singh and Raman [9] presented a copy-move image forgery detection scheme based on radix-sort and eventually used the radix-sort to carry out lexicographic sorting on the feature vectors, result from the work indicates that radix-sort is faster and enhances computational complexity involved in the sorting process. Therefore, the speed of lexicographical sort can be enhanced if hybridized with radix-sort technique. Also, mapping is performed to vividly identify forged regions in an image, this can be achieved by colorings forged regions in order to differentiate them from the un-tampered regions [5]. The block-based techniques are categorized into six including frequency transformation, textual and intensity, moment invariant, dimension reduction, multi-scale auto-convolution, and other proposed block-based division methods:

1) Frequency Transformation

Frequency transformation is a technique for feature extraction known to be robust against noise adding and geometric transformation operations. It is the most commonly used block based feature extraction technique, and can be further divided into various methods for detection such as discrete cosine transformation (DCT), discrete wavelet transformation (DWT) and dyadic wavelet

transformation (DyWT) and hybridized DCT and DWT. The details of each of these techniques are discussed in subsequent subsections.

a. Discrete Cosine Transformation

The discrete cosine transformation (DCT) segments the image into spectral sub-bands of varying importance. Images can be transformed from the spatial domain to the frequency domain using the DCT technique. Cao *et a*l. (2012) used a block based method, the current discrete cosine transformation (DCT) was improved and the dimension of the feature vector was reduced thereby reducing the computational complexity. Discrete cosine transforms (DCT) and Gaussian RBF kernel PCA technique was proposed by Mahmood *et a*l. (2016a) to solve the issue of increased dimensional nature of the feature space. Rather than extracting sparse features that give results that are less accurate, Bi *et a*l. proposed a dense-field method based on DCT to extract features from the suspected image and afterwards, a new matching method based on the features extracted by colour texture descriptors and invariant moments descriptors is performed, and this solves the issue of high computational complexity resulting from using the dense-field approach. However, Ustubioglu *et a*l. (2016), used DCT and element by element matching technique in the detection of copy-move forgery detection.

b. Discrete Wavelet Transformation

Discrete wavelet transformation **(**DWT) technique was adopted by Zhang [10] and Feng [11], to achieve reduction in features dimension, but a dis-advantage a this technique is its reliant on the position of copy-move region within an image, for instance, if a copy-moved region falls within more than one sub-divisions of an image, therefore, these sub-divided images must be divided into smaller blocks and the process of localizing the copy-moved parts must be repeated.

c. Dyadic Wavelet Transformation

DyWT is known to be a more suitable technique for the analysis of data due to its shift invariant nature. A method based on un-decimated dyadic wavelet transform was proposed by Muhammad Hussain [12] using LL1 and HH1 sub-bands to find the correlation and differences between image blocks, so as to expose the presence of copy-move forgery.

d. Hybridization of DCT and DWT

When DCT is used solely for image forgery detection, it is likely to expose wrong blocks due to various reasons such as large dimensionality of suspected image and similarity between two or more blocks. Hayat and Qazi [13] proposed a method, hybridizing DCT and DWT. DWT complements the short comings of DCT by firstly reducing the image size without tampering with the appropriate features for localizing forged regions, afterwards, image will be divided into blocks and DCT will be applied to extract relevant features.

2) Texture and Intensity

Texture and intensity technique leverage on features such as smoothness, roughness and uniformity of the texture content of an image and extract these features to detect duplications in the image. Information about the intensity of an image can be found in the CPU and GPU engine. However, it is a known fact that the processing time for analysis with GPU engine is twelve times more than the CPU. Based on this, Singh and Raman [9] proposed a scheme which utilizes radix sort technique by embedding it into the GPU engine rather that CPU to achieve an enhanced copy-move forgery detection scheme. Texture information of an image can also be extracted using a technique known as the Local Binary Pattern (LBP), this feature extractor is one of the most preferable technique used by researchers because its computational complexity is low [14]. Several variants of LBP such as multi-resolution LBP (MLBP) [8], centre symmetric LBP (CSLBP) and LBPROT has been proposed thereafter. Ulutas, Ustubioglu [15] used the local binary pattern (LBPROT) technique which is invariant to rotation to extract texture information from an image, however, this technique is very effective in detection of forgery involving tampering on smooth regions.

3) Moment Invariant

Moments invariant are known to possess features that are robust against post-processing operations such as scaling, rotation and transformation. Efforts have been made by various researchers towards improving on the features of standard moments, as a result, innovations such as central moment, Blur invariant moment, Krawtchouk's moment, Zernike moment and exponential moment were proposed. Blur invariant moment is robust against total contrast transforms, noise addition and blur deterioration. When moment invariant features are extracted from an image with large dimensionality, it results to an increase in computational complexity, to solve this problem Kashyap and Joshi [16] proposed a method that combines blur moment with DWT. Also, Zernike moment is resistant to rotation operation and noise but not robust against scaling and other affine-transformation based forgery operations, based on this, Zhong and Xu [17] combined a form of central moment which is known as histogram-invariant moment with exponential moment to achieve an improvement in computational duration and resistant to scaling, rotation and contrast transforms. However, Krawtchouk’s moment is invariant to most forms of post-processing operations, especially Gaussian blurring and possess the ability to expose tampering in regions having non-uniform shape [18].

4) Dimension Reduction

Dimensionality of an image can also be reduced by applying a technique for dimension reduction, some of these techniques include, Singular Value De-composition (SVD) and Locally Linear Embedding (LLE). SVD is known to be invariant to rotation, scaling and noise, but a downside of SVD is its inability to extract sufficient features which can lead to missing image information and as a result, yields low performance while LLE is an effective technique for dimensionality reduction of a large sized image dataset [19]. As compared to LLE, SVD has the highest resistance to varieties of post-processing attacks and reduced processing cost [5].

5) Multi Scale Auto-convolution

MSA is a feature extraction technique for block based method which known by its resistance to affine change and vector sequence and is robust against post-processing attacks such as rotation, noise adding and jpeg compression but not robust against scaling. In Wang, Tang [20] a method based on MSA was proposed, the MSA vector sequence which is a four dimensional eigenvector is extracted from each block in an image. The proposed method was found to be effective in its robustness against post-processing operations and possess reduced computational time.

6) Other Proposed Block Based Division Methods

However, a blind forensic approach which is based on histogram of oriented gradient was used by Lee, Chang [21] in the detection of copy-move forgery in images. However, due to the fact that many methods detect a copy move forgery of dimension not below 16 × 16, Sharma and Ghanekar [22] proposed a method which uses a centre symmetric local binary pattern (CSLBP) and can detect forged medical images with a 12 × 12 dimension. Lee [23] also proposed a method to detect and precisely locate different types of copy-move forgery within the same image by using the Histogram of Gabor Magnitude (HOM) which is based on the block wise division method. In Isaac and Wilscy [24], Gabor wavelet and Local Phase Quantization (LPQ) was used to determine if an image is authentic or forged and to localize the forgery. Difficulty in the detection of removed object from an image using image-inpainting to prevent any trace was addressed in Liang, Yang [25], the proposed method integrates Central Pixel Matching (CPM), Greatest Zero Connectivity component Labelling (GZCL) and Fragment Splicing Detection (FSD).

III. The Proposed Method

In this section we outlined design and development process of the copy move image forgery detection scheme using DCT technique, which is presented as follows. First, an illustration of the detection scheme is presented. Then, technique for image splitting is analysed. Thereafter, a detailed discussion on the feature extraction process is given. Also, the process for feature matching is presented. Conclusively, the method used in determining the appropriate sorting technique for the proposed scheme is described.

A. DCT Based Copy Move Forgery Detection (CMFD) Framework

Illustrated in Fig. 1 is an architecture of the DCT based image copy-move forgery detection scheme. As compared with previous detection techniques, the proposed method is slight different with respect to an improvement in the feature extraction process. First, the image is converted to grayscale, in case it is a coloured image. Next, the suspicious image is divided into blocks of 16 × 16 pixels and the DCT coefficients are extracted by applying DCT to the image block. Afterwards, the dimension reduction which is based on an octagonal shape must be performed on the extracted DCT coefficients to output the dimensionally reduced DCT coefficients. To identify similar block pairs, the dimensionally reduced DCT coefficient must be sorted for each block of 16 × 16 pixels. The identified matching pairs represent the copy-pasted regions. The following steps are employed for the CMFD framework:

1) Colored Image Conversion to Grayscale

Since a colored image consists of RGB (red, green and blue) components, the Y' which is known as the luma channel needs to be separated from the RGB component. This process is essential for DCT to extract features from the obtained grayscale image. In Welsh, Ashikhmin [26], the equation showing the process of calculating Y' was give. This process is shown in Eq. 1.

$$Y' = K_R \cdot R' + (1 - K_R - K_B) \cdot G' + K_B \cdot B' \quad (1)$$

2) Image Splitting

Suspicious image is divided into fixed size blocks of 16 × 16 pixels. This implies that the arrangement of the blocks consists of rows and columns. Hence, N_{blocks} of overlapped sub-blocks will be obtained from the suspect image in Eq. 2.

$$N_{blocks} = (M - B + 1) \times (N - B + 1) \quad (2)$$

3) Feature Extraction

After dividing the suspicious image into fixed size blocks of 16 × 16 pixels, since DCT cannot be applied directly on the block of 16 × 16 pixels of this image, therefore the multiple dimensional vector must be converted to a one-dimensional vector by concatenating all the rows into one row, which implies a vector length of 1 × 256 pixels, afterwards the DCT can be applied on the concatenated pixels to extract the quantized coefficient of the segmented image. Definition of DCT of a given B × B pixel matrix is shown in Eq. 3.

$$DCT(i,j) = \frac{1}{\sqrt{2N}} C(i)C(j) \sum_{x=0}^{N-1} \sum_{u=0}^{N-1} pixel(x,y) Cos\left(\frac{(2x+1)i\pi}{2N}\right) Cos\left(\frac{(2y+1)j\pi}{2N}\right) \quad (3)$$

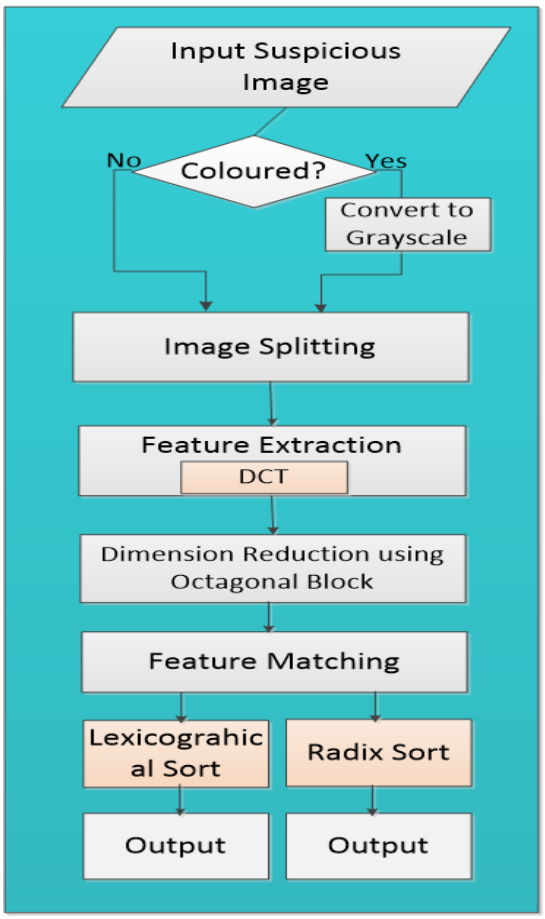

Fig. 1. Copy-Move Image Forgery Detection Scheme

4) Dimensional Reduction

To perform the dimension reduction operation, each quantized block needs to be represented by an octagonal block, and while representing the quantized block in an octagonal shape, the indices of each block within the octagon needs to be obtained because some pixels appears to fall in between the octagonal block region and the region outside the octagon as shown in Fig. 2. Therefore, these pixels in-between the desired region and the unwanted region can either be added or removed from to desired region. In this work, removing the pixels is considered. Then, the vector containing only the desired indices will be obtained and will afterward be applied in the feature matching stage.

5) Feature Matching

Prior to the feature matching stage, the feature extraction and dimension reduction operations need to be repeated on each block of 16 × 16 pixels and this process will be iterated until the whole region has been covered. After the iterated operation has been performed, each 16 × 16-pixel block is sorted. The pixels will be arranged in ascending order base on their values, in this process the matching pixels come closer to each other. Pixels with the same values are matched and therefore, represent the copy-moved regions.

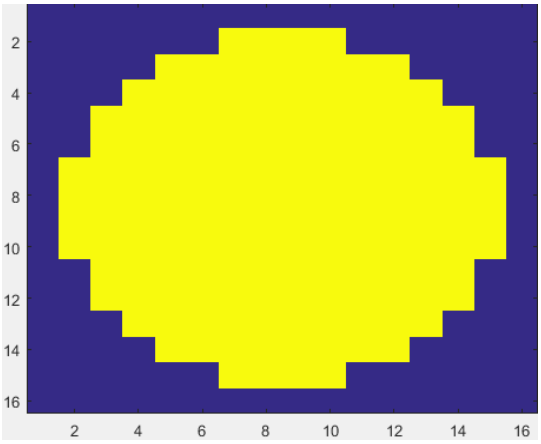

Fig. 2. Pixels Captured Within the Shape

6) Matching with Radix Sort

Radix sort is a non-comparative integer sorting algorithm that sorts data with integer keys by grouping keys by the individual digits which share the same significant position and value. Radix sort performs its operation by sorting from the least significant digit instead of most significant digit. This process is much better than sorting by most significant digit because it saves having to keep track of multiple sort jobs.

7) Matching with Lexicographical Sort

Lexicographical sort entails ordering a matrix in a way that similar vectors are moved closer. Each feature vector is compared to next vectors, afterwards a calculation of the Euclidean distance is performed. If the calculated distance is less than the set threshold, there exist a shift vector in-between the upper coordinates of the corresponding blocks which will be calculated. If the calculated shift vector is higher than the set threshold, the blocks which lies within these vectors are identified as tampered regions.

IV. Result And Analysis

The following result (Fig. 3,4,5 and 6) are obtained after applying and implementing our methodology in section three that is, our proposed work. Haven completed all the steps mentioned previously, the forged regions on the image are exposed, and this represents the final detection results. Tampered areas can be known by marked regions on the resulting image which indicates forgery as shown in Fig. 3,4,5 and 6. Successful detection can also be judged by comparing the forged image results with the original image in the dataset.

V. Conclusion

In this paper, we have studied the copy-move image forgery detection based on their techniques and approaches. Further, the CMFD frameworks has been designed and developed for the image forgery detection considering DCT approach. The detection obtained on the image shows the significance of our CMFD framework based on its

performance and represent 85% of the quantized DCT coefficients on each image block and achieve improved accuracy and minimal computational complexity. Hence, we conclude that the detection scheme proposed is feasible and efficient for medical image forgery detection.

Fig. 3. Original Medical Image

Fig. 4. Tampered Medical Image

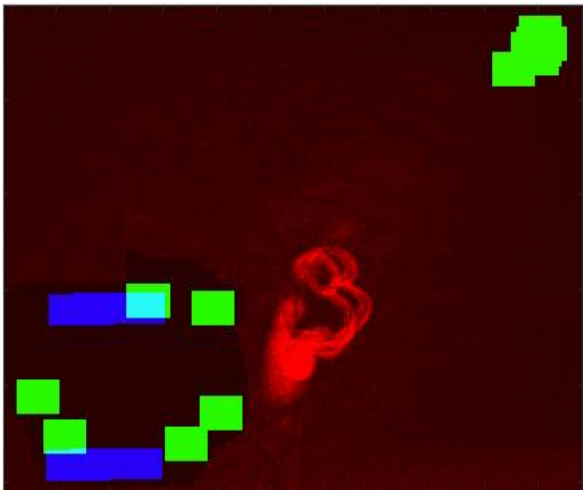

Fig. 5. Initial Detection Result on Tampered Image

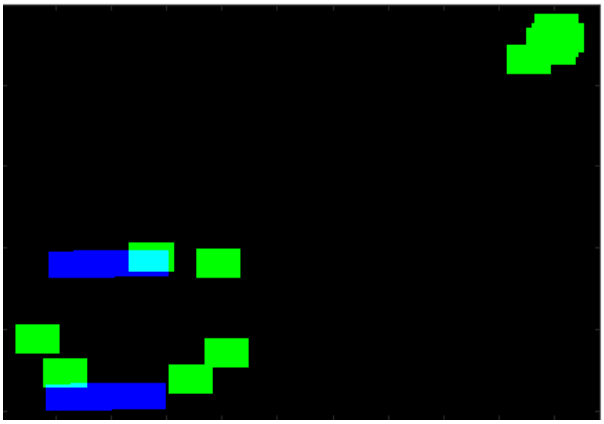

Fig. 6. Tampered Regions

ACKNOWLEDGMENT

The research is supported by Ministry of Education Malaysia (MOE), Cyber Security X-Lab UTM Malaysia and conducted in Collaboration with Research Management Centre (RMC) at Universiti Teknologi Malaysia.

REFERENCES

[1] Kakar, P., N. Sudha, and W. Ser. (2011). Exposing digital image forgeries by detecting discrepancies in motion blur. *IEEE Transactions on Multimedia*, 13(3), 443-452.

[2] Jaberi, M., *et al*. (2014). Accurate and robust localization of duplicated region in copy–move image forgery. *Machine Vision and Applications*, 25(2), 451-475.

[3] Warif, N. B. A., *et al.* (2016). Copy-move forgery detection: Survey, challenges and future directions. *Journal of Network and Computer Applications*, 75, 259-278.

[4] Mahmood, T., *et al*. (2016). copy-move forgery detection technique for forensic analysis in digital images. *Mathematical Problems in Engineering*, 2016, 1-13.

[5] Cao, Y., *et al.* (2012). *A robust detection algorithm for copy-move forgery in digital images. Forensic Science International*, 214(1), 33-43.

[6] Davarzani, R., *et al.* 2013. *Copy-move forgery detection using multiresolution local binary patterns. Forensic Science International*, 231(1), 61-72.

[7] Singh, J. and B. Raman. (2012). *A high performance copy-move image forgery detection scheme on GPU. Proceedings of the International Conference on Soft Computing for Problem Solving (SocProS 2011) December 20-22, 2011*. Springer.

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

[9] Muhammad, G., M. Hussain, and G. Bebis. (2012). Passive copy move image forgery detection using undecimated dyadic wavelet transform. *Digital Investigation*, 9(1), 49-57.

[10] Hayat, K. and T. Qazi. (2017). Forgery detection in digital images via discrete wavelet and discrete cosine transforms. *Computers & Electrical Engineering*.

[11] Ojala, T., M. Pietikäinen, and D. Harwood. (1996). A comparative study of texture measures with classification

based on featured distributions. *Pattern Recognition*, 29(1), 51-59.

[12] Ulutas, G., *et al.* (2017). Medical Image Tamper Detection Based on Passive Image Authentication. *Journal of Digital Imaging*, 1-15.

[13] Kashyap, A. and S. D. Joshi. (2013). Detection of copy-move forgery using wavelet decomposition. *Signal Processing and Communication (ICSC), 2013 International Conference on*. IEEE.

[14] Zhong, L. and W. Xu. (2013). A robust image copy-move forgery detection based on mixed moments. *Software Engineering and Service Science (ICSESS), 2013 4th IEEE International Conference on*. IEEE.

[15] Imamoglu, M. B., G. Ulutas, and M. Ulutas. (2013). Detection of copy-move forgery using krawtchouk moment. *Electrical and Electronics Engineering (ELECO), 2013 8th International Conference on*. IEEE.

[16] Junhong, Z. (2010). *Detection of copy-move forgery based on one improved LLE method*. in *Advanced Computer Control (ICACC), 2010 2nd International Conference on*. IEEE.

[17] Wang, T., *et al.* (2012). Blind detection of copy-move forgery based on multi-scale autoconvolution invariants. *Chinese Conference on Pattern Recognition*. Springer.

[18] Lee, J.-C., C.-P. Chang, and W.-K. Chen. (2015). Detection of copy–move image forgery using histogram of orientated gradients. *Information Sciences*, 321, 250-262.

[19] Sharma, S. and U. Ghanekar. (2015). *A Rotationally Invariant Texture Descriptor to Detect Copy Move Forgery in Medical Images*, 795-798.

[20] Lee, J.-C. (2015). Copy-move image forgery detection based on Gabor magnitude. *Journal of Visual Communication and Image Representation*, 31, 320-334.

[21] Isaac, M. M. and M. Wilscy. (2015). image forgery detection based on gabor wavelets and local phase quantization. *Procedia Computer Science*, 58, 76-83.

[22] Liang, Z., *et al.* (2015). An efficient forgery detection algorithm for object removal by exemplar-based image inpainting. *Journal of Visual Communication and Image Representation*, 30, 75-85.

[23] Welsh, T., M. Ashikhmin, and K. Mueller. (2002). Transferring color to greyscale images. *ACM Transactions on Graphics (TOG)*. ACM.