

# Polar Coordinate and Discrete Wavelet-Based Approach For Copy-Move Forgery Detection

S. Devi Mahalakshmi\* and K. Vijayalakshmi

Mepco Schlenk Engineering College, Sivakasi, India

Received: 23 May 2019, Revised: 3 Jul 2019, Accepted: 7 Jul. 2019

Published online: 1 Aug. 2019

**Abstract:** In recent years, digital images have become prevalent in all transactions of all organizations. Many governmental, legal, scientific, and news media organizations rely on digital images to make critical decisions or to use them as a photographic evidence of specific events. The digital image forgery is the process of manipulating the original photographic images to create the forged image. With the availability of powerful image editing tools, numerous image retouching techniques have become practical. Not all such image editing and alterations are harmful. However, malicious-intended modification of image content forms a serious threat to the secure and legal usage of digital images. Hence, there is a great need for digital forensic techniques which could detect such image alterations, forgeries and authenticate the images. The proposed method focuses on copy-move forgery detection using polar coordinate and discrete wavelet-based approaches. In polar coordinate approach, the image is divided into overlapping blocks and each block is converted into polar from which features are extracted. In discrete wavelet-based approach, wavelet-transformed image is divided into overlapping blocks and features are extracted. For similarly matching of blocks correlation coefficients are used. Experiments are conducted on the dataset provided by DVMM Columbia university for copy-move forgery detection.

**Keywords:** Image forgery, wavelet, block division; polar coordinate, discrete cosine transform, fourier transform, correlation

## 1 Introduction

In the digital era, digital image are commonly used as substantial evidence of a crime, hence digital image provides assistance for making judgment about a criminal event. Nowadays digital image forgery becomes inescapable with the use of easy access of powerful image editing software tools like Photoshop, 3D Max, GIMP etc. Hence it grows increasingly hard to rely on originality of image, and it becomes a challenging problem. So many researches focused on the techniques to examine the originality and authenticity of digital images.

Copy-move forgery is one of the most popular image forgery [1,2,3,4,5,6,7] techniques because it can be done in ease and perfectly with freely available image editing tools. The main objective of copy-move image forgery is to cover the details of evidence or to duplicate some extra regions in the images to deviate the judgment. Here part of same image is copied and pasted into another region of the image to remove or hide the original evidence. Since the altered images look natural, it is very hard to detect such forgeries with naked eyes. Hence there is a need for powerful and efficient forgery detection method to detect

such copy pasted and replicated regions, even though they are slightly dissimilar to originals. Image processing techniques and advanced machine learning algorithms [11,12,13,14,15] can be integrated to solve issues into the images [8,9,10].

Hasmi MF et al., [16] proposed a method based on SIFT and DWT. The DWT is used for dimensionality reduction. DWT is applied on the image, which decomposes the image into four parts as LL, LH, HL, and HH. As the LL part of the image alone contains most significant information, they extract the SIFT features from the LL part alone. From the extracted SIFT features; key descriptor vectors are derived from which we can find similarities between various descriptor vectors. The main advantage of this method was its high accuracy as compared to other methods and reduced computation complexity. It divides the image into four parts and only one part is used for further processing, the efficiency of the algorithm depends upon the image size.

\* Corresponding author e-mail: [osdevi18@gmail.com](mailto:osdevi18@gmail.com)

Saiqa Khan and Arun Kulkarni et al., [17] proposed copy-move image forgery detection using wavelet approach. In this technique, usage of wavelet transform for compression has been tested and phase correlation is used as similarity checking criterion for identifying duplicated overlapping blocks formed. This is done through two phases. The first phase deals with the detection of reference and matching on the lowest level of wavelet transform compressed. For this, matrix is sorted and correlation is calculated with row order relation. However this technique is good at detecting more complex images but cannot be used for detecting forgery with rotation and scaling.

Diaa M. Uliyan et al., [18] proposed a method for copy-move image forgery detection using Hessian and center symmetric local binary Pattern. This method consists of four steps. The first step is detects the object based on normalized cut segmentation, and the second step is localizes the local interest points of each object based on the Hessian method, and the third step extracts CSLBP features, and the last step is detects duplicated regions in forged images. From the experiment results they proved that this approach is robust to post processed copy-move forgery under geometric transformation such as scaling, and JPEG compression.

Jian Li et al., [19] presented a copy-move forgery detection scheme based on image segmentation. In this method, an image is segmented into semantically independent patches, such that the copy-move forgery detection can be done by partial matching among those segmented patches. The matching process between segmented patches consists of two stages where an accurate estimation of transform matrix can be obtained by an EM-based algorithm and matched.

B. Mahdian et al., 2007 proposed the Principal Component Analysis (PCA) dimensionality reduction-based technique [20], for image forgery detection. This approach is similar to DCT method with improvement in capturing discriminating features. In this approach the original image was transformed into grayscale and separated into blocks. These parts or blocks are prearranged in lexicographical order in earlier matching then PCA is used to represent the dissimilar blocks in a substitute mode. This method adept for detection even if there is involved minor image alteration due to noise or lossy compression. However this technique is meant for grey scale images only and also processes every color channel using PCA for the detection of counterfeits. This method shows better performance in detecting copy-move forgeries with less number of false positives.

M. Sridevi et al., 2012 proposed a method that uses complete copy-move forgery detection for real-time [21] images. In such cases other previous approaches exhibit

high computation time and they are not suitable for real time applications. The proposed approach separated the grayscale image into many overlapping blocks of a predefined size and then intensity features are extracted for every block. In this method the performance is proved to be better than other conventional techniques. This approach also controls the false detection rate through the adjustment of the block size, but this method has its own limitation and is not suitable for color images.

Junwen Wang et al., [22] proposed an efficient and robust algorithm for the detection of a specific type of image forgery known as region duplication, which is done by copying a block of an image and pasting into to other regions of the same image. Here the dimension of the image is reduced by Gaussian pyramid, then the image is split into regions of circular blocks with four extracted features for each circle block. Then the feature vectors are lexicographically sorted and similarity matching was done using area threshold value. Experimental results proved that this method is robust to the post processing such as noise addition, blurring, lossy compression.

Z.Mohamadian et al., 2013 introduced two methods [23]; DWT (Discrete Wavelet Transform) and KPCA (Kernel Principal Component Analysis) for copy-move forgery detection. In this method, the image is separated into many parts and for every block DWT vectors and KPCA-based vectors are calculated. After this calculation these vectors are sorted lexicographically and the related points are searched to intend their offset frequencies. This approach is developed for detecting the rotation type and flip of forgeries, geometric transformation using labeling technique. This approach has better performance than the conventional PCA approach. Further, it is used to detect forgeries, even in images with lossy JPEG compression and with additive noise.

Gul Muzaffer et al., [24] proposed copy-move forgery detection based on Gabor filter and ORB. In this work, there are four basic steps involved as follows: i) Extraction of the texture information from forged image with Gabor filter and then histogram equalization. ii) Extraction and detection of the ORB keypoints and descriptors from the textured image. iii) Matching of the keypoints to locate forged regions with Hamming distance. iv) RANSAC approach for the removal of false match. Here, the forgery detection capability of the proposed method is tested with a metric called Detection Ratio (DR). This work has achieved better accuracy in detecting image forgery with higher DR.

The proposed work in this paper is organized as follows. Section II presents the different modules involved in forged region detection. Section III provides experimental results on forgery detection and Section IV narrates conclusions.

## 2 Proposed Method

The architectural design for forged region detection in digital images is shown in Figure 1, which follows two methods. The first method (left-hand side of the Figure) which is method-1 polar coordinate based approach, the input image is converted into grey scale image. Then the grey image is divided into overlapping blocks and each block is converted into polar block, where the translation, scaling transformations resulted in shifting. After that, Fourier coefficient features are extracted from each polar block to form the feature vector. Then, the feature vector gets sorted and matched to find the similar blocks using correlation coefficient. In the second method (right-hand side) which is method-2, the input image is converted into grey scale image. Then discrete wavelet transformation is applied, where the image is divided into four sub-bands (LL, LH, HL, HH). From these sub-bands, LL alone is taken for further processing since it has most significant information. Then, LL part is divided into overlapping blocks. After that, Discrete Cosine Transform (DCT) features are extracted to form the feature vector. Then, matching of blocks is done using correlation coefficient.

**Preprocessing:** The input color image is converted into gray-scale image and subjected to the noise removal. The various task involved in the forgery detection using polar coordinate-based approach are explained as follows:

**A1 Block Division:** The gray image of size  $M \times N$  is divided into overlapping blocks with block size as 8.

**A2 Polar block Conversion:** Each block in the image is converted into polar block. When converting the image block into polar block, any transformations like translation and rotation in Cartesian representation results as shifting in polar representation. That is,  $(a, b)$  is the coordinate of point in Cartesian plane which is transformed to  $(r, \theta)$  in polar form where,  $r = \sqrt{a^2 + b^2}$  is the magnitude and  $\theta$  is the angle given by  $\arctan(a/b)$  as shown in Figure 2.

**(A3) Feature Extraction:** From each column of the block, Fourier transform coefficients are extracted and stored as row major order, where the input image is in spatial domain representation and the output of the transformation represents the image in frequency domain. For a square image of size  $N \times N$ , the two-dimensional DFT is given by equation (1).

$$F(k, l) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} f(i, j) e^{-2\pi i \left( \frac{ki}{N} + \frac{lj}{N} \right)} \quad (1)$$

where  $f(a, b)$  is the image in the spatial domain and the exponential term is the basis function corresponding to each point  $F(k, l)$  in the Fourier space. The equation can be interpreted as: the value of each point  $F(k, l)$  is obtained by multiplying the spatial image with the corresponding base function and summing the result.

The various task involved in the forgery detection using discrete wavelet-based approach are explained as

follows:

**B1 Wavelet Transformation:** DWT is applied to the gray-scale image which results into  $3l+1$  sub-bands. From these sub-bands, lower frequency sub-band which has the size of order  $\frac{n}{2} \times \frac{n}{2}$  is taken for further processing where,  $n$  is the square image of size  $n \times n$  and the remaining bands are ignored. Discrete wavelet transform accommodates simultaneous frequency and spatial domain information of the image. Here the image is analyzed by the sequence of analysis filter bank and decimation operation involved while applying DWT. The analysis filter bank consists of a pair of high and low pass filters which depends upon each decomposition level. The low pass filter removes the approximate information of the image but the high pass filter removes the details such as edges.

**B2 Block Division:** For an image of size  $M \times N$ , the pre-processed image is divided into small fixed-size overlapping blocks of size  $b \times b$  pixels. The calculation of resultant blocks  $B$  where shown in equation (2),

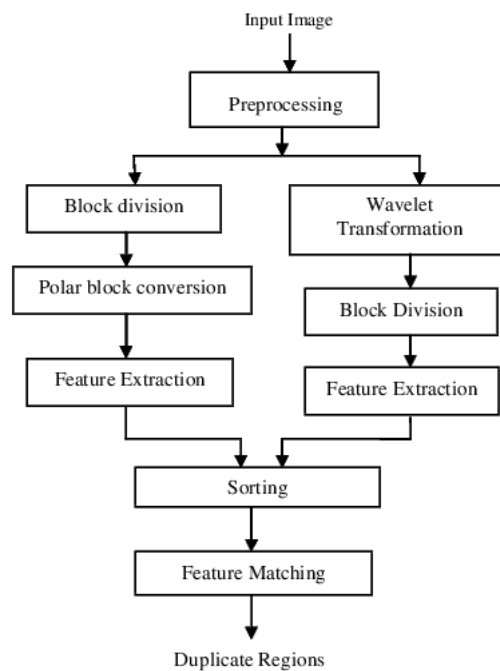
$$B = (M - b + 1)(N - b + 1) \quad (2)$$

**B3 Feature Extraction :** Discrete cosine transform is applied to each individual blocks and the most energetic of coefficients are extracted from each block to form the feature vector. The DCT is a Fourier-related transform that is the Discrete Fourier Transform (DFT), but uses only real numbers. In general the DCTs are generally related to Fourier Series coefficients of a periodically and symmetrically extended sequence whereas DFTs are associated with Fourier series coefficients of a periodically-extended sequence. DCTs are equivalent to DFTs of roughly twice the length, operating on real data with even symmetry (since the Fourier transform of a real and even function is real and even), whereas in some variants the input and/or output data are shifted by half a sample.

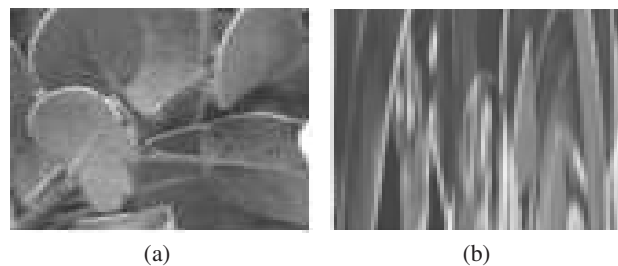
**C. Lexicographical Sorting:** The feature vector is in the form of matrix which contains  $n$  elements and indices of block position where  $n$  represents the number of elements in the block. Each row represents the blocks. It is lexicographically sorted, so that blocks with similar features become closer to each other and also block position sorted accordingly to form is sorted feature matrix. While sorting, the rows are sorted based on the ascending order according to the first column. If the first column contains the repeated elements, then it sorted based on the second column and this process repeats.

**D. Feature Matching:** The sorted feature matrix is matched using correlation coefficient. Each block  $i$  needs to be compared with each block  $j$  ( $j \neq i$ ) to get the correlation coefficients of the form  $\rho_{ij}$  as shown in Equation 3, we end up with a total of  $k(k-1)/2$  correlation coefficients. Correlation Coefficient values are between -1 to +1. Finally, we map the duplicated blocks by comparing all the  $\rho_{ij}$  to a positive threshold  $\rho_0$ .

$$\rho_{ij} = \frac{\sum_{i=1}^n (x_i - \bar{x}) \cdot (y_i - \bar{y})}{\sqrt{\sum_{i=1}^n (x_i - \bar{x})^2 \cdot \sum_{i=1}^n (y_i - \bar{y})^2}} \quad (3)$$



**Fig. 1:** Image forgery detection.



**Fig. 2:** Cartesian representation (left) and polar representation (right).

Where,  $(\bar{x}, \bar{y})$  - blocks FT coefficients  $(\bar{x}, \bar{y})$  is the mean value of  $x, y$ , respectively, and  $n$  is the number of coefficients in the block.

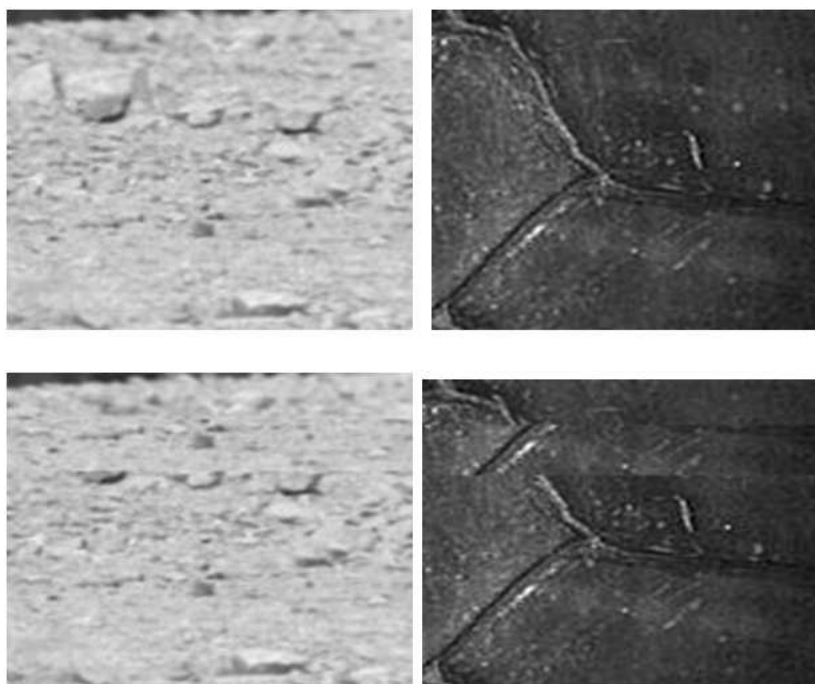
### 3 Experimentation and Results

Experiments have been conducted on the dataset provided by DVMM, Columbia University, which consists of images of size 128 x 128. These dataset provides images with small duplicated regions with repetitive patterns which are required to create forgery content using post-processing operation such as blurring, and additive noise.

In comparing Table 4 and Table 5, the precision rate is higher when applying Haar wavelet. And also, the

execution time is less for Haar wavelet than the Daubechies as shown in Table 6. While comparing the two methods, method-1(Polar coordinate-based approach), has higher accuracy than the method-2 (Discrete wavelet-based approach), for copy-move forgery detection as shown in Table 7. In method-1 (polar coordinate based approach), the block size used for the experimentation is 8 X 8. Therefore, the number of blocks created is 14640 blocks. Since the block size is 8, the number of elements contained in each block is 64. Number of blocks =  $(M-B+1)*(N-B+1)$   
 $= (128-8+1)*(128-8+1)$   
 $= 121*121$   
 $= 14641$

Here Fast Fourier Transform (FFT) is performed to each column in the block and stored as the row vector. All



**Fig. 3:** Sample images from DVMM dataset. Original image (top) and forged image (bottom).

**Table 1:** Confusion matrix with different correlation threshold (Using FT as a feature).

T	Detected	FP	TP	FN	TN	Precision P
1	1694	0	1694	0	12,947	<b>1</b>
0.99	1728	34	1694	0	12,913	<b>0.98</b>
0.98	3133	1439	1694	0	11,508	<b>0.54</b>
0.97	4256	2562	1694	0	10,385	<b>0.4</b>
0.96	5177	3483	1694	0	9,464	<b>0.32</b>
0.95	6008	4314	1694	0	8,633	<b>0.28</b>

the blocks feature vectors are stored in a feature matrix A of size  $B \times n$ , where each row is considered as a block feature and the number of rows refers to the number of blocks B and n represents the number of elements in each block. Therefore, the size of the feature vector is  $14641 \times 64$ .

In method-2 (discrete wavelet-based approach) the gray scale image is subjected to level l DWT to get  $3l+1$  sub-bands. Therefore the sub-bands formed are LL, LH, HL, HH with  $l=1$ . LL is taken for further processing which is of size  $64 \times 64$ . Figure 4 shows the four sub-bands of image after applying wavelet transform.

By comparing Table 1 and Table 2, the precision rate is higher while extracting Fourier coefficient (FT) than the DCT coefficient-based approach. But the execution time is less for DCT-based scheme than the FT-based approach as shown in Table 3. The precision rate achieved

for different threshold value by applying Haar wavelet is shown in Table 4.

The number of blocks formed is

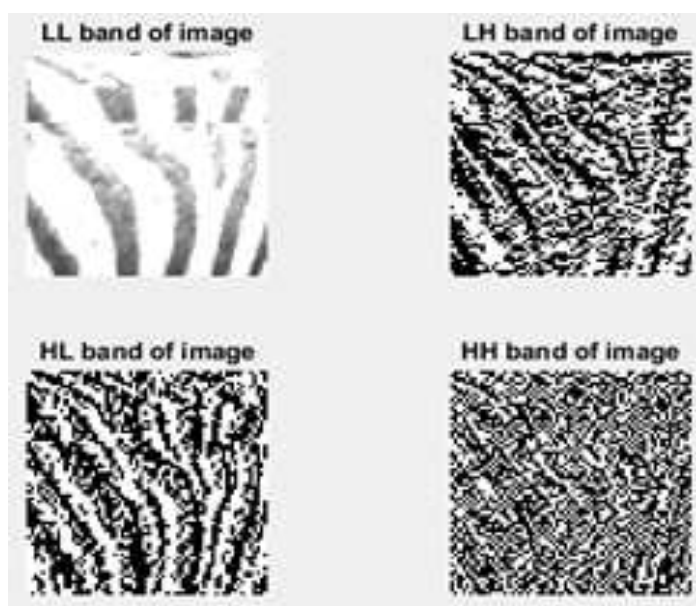
$$\text{Number of blocks} = (M-B+1) \times (N-B+1)$$

$$= (64-8+1) \times (64-8+1)$$

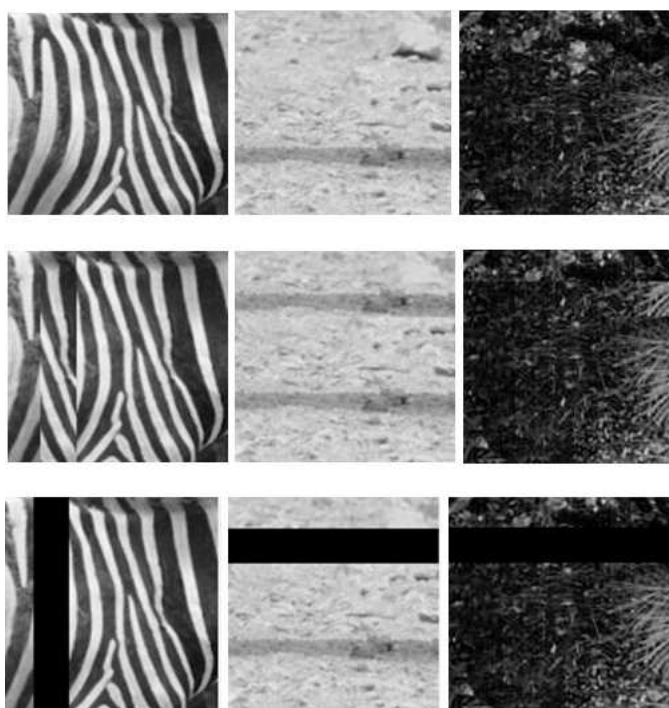
$$= 57 \times 57$$

$$= 3249$$

DCT is applied to each individual block to form the feature matrix. Each row in the feature matrix denotes the number of blocks. Then, the feature matrix gets sorted to obtain the similar blocks. Therefore, the size of feature matrix is  $3249 \times 64$ . Figure 5 shows the result of copy-move forgery detection for few sample images taken.



**Fig. 4:** Four sub-band of a sample image.



**Fig. 5:** Original image (top), forged image (middle) and Result of copy-move forgery detection (bottom).

**Table 2:** Confusion matrix with different correlation threshold (Using DCT as a feature).

T	Detected	FP	TP	FN	TN	Precision P
1	1694	0	1694	0	12,947	<b>1</b>
0.99	1761	67	1694	0	12,880	<b>0.96</b>
0.98	13271	11577	1694	0	1370	<b>0.13</b>
0.97	14293	12599	1694	0	348	<b>0.12</b>
0.96	14551	12857	1694	0	90	<b>0.14</b>
0.95	14598	12904	1694	0	43	<b>0.16</b>

**Table 3:** Average execution time of polarcoordinate-based approach.

Number of Images	POLARCOORDINATE BASED METHOD	
Feature Extraction	FT(sec)	DCT(sec)
Single Image	44.496	31.4985
180 Images	3974.89	2478.5687

**Table 4:** Confusion matrix with different correlation threshold (using Haar wavelet).

T	Detected	FP	TP	FN	TN	P
1	171	0	171	0	3078	<b>1</b>
0.99	211	40	171	0	3038	<b>0.81</b>
0.98	261	90	171	0	2988	<b>0.65</b>
0.97	327	156	171	0	2922	<b>0.52</b>
0.96	414	243	171	0	2835	<b>0.41</b>
0.95	496	325	171	0	2753	<b>0.34</b>

## 4 Performance Evaluation

For experiments, in method-1, images with 14641 blocks have been tested. The number of positive blocks that are correctly identified is around 1694 blocks while the negative blocks are 12,947 blocks. Here Precision P as shown in equation (4) is used to measure the detection accuracy rate. Table 1 shows the precision rate with FT as a feature vector for different correlation threshold values and Table 2 shows the precision rate for DCT coefficients as a feature.

$$\text{Precision, } P = \frac{TP}{TP + FP} \quad (4)$$

## 5 Perspective

The proposed work is used to detect the copy-move forged images and also detects the image region where forgery is involved. In polar coordinate-based method to find the forged region, the given image is preprocessed and divided into overlapping blocks. Then, each block is converted into polar block and Fourier coefficients are

extracted. Then block matching is done using correlation coefficient. In discrete wavelet-based method, given forged image is preprocessed and divided into overlapping blocks. Then, from each block DCT coefficients are extracted and sorted. After that, the similarity of blocks is found by correlation coefficient. From the experiments results, it is concluded that though the precision rate of polar coordinate-based approach increases while using FT coefficient, the execution time is better for DCT based approach. The DWT approach using Haar wavelet is efficient when compared to Daubechies wavelet. While comparing both methods, the polar coordinate-based approach exhibits high accuracy than the DWT-based approach.

## Acknowledgement

The authors immensely thank the Management and Principal of Mepco Schlenk Engineering College, Sivakasi for their full support to carry out this research work.

**Table 5:** Confusion matrix with different correlation threshold (using Daubechies wavelet).

T	Detected	FP	TP	FN	TN	P
1	0	0	171	0	3,078	<b>1</b>
0.99	21	156	171	0	2,922	<b>0.52</b>
0.98	90	791	171	0	2,287	<b>0.17</b>
0.97	188	1570	171	0	1508	<b>0.09</b>
0.96	2092	1921	171	0	1157	<b>0.08</b>
0.95	2301	2130	171	0	948	<b>0.07</b>

**Table 6:** Average execution time of discrete wavelet-based approach for copy-move forgery detection.

Number of Images	<b>DISCRETE WAVELET BASED METHOD</b>	
Feature Extraction	<b>Haar (sec)</b>	<b>Daubechies(sec)</b>
Single Image	0.5243	1.3641
180 Images	114.0213	130.2133

**Table 7:** Comparison of polar coordinate and discrete wavelet-based approaches.

	<b>Total Images</b>	<b>Correctly Identified</b>	<b>Accuracy (%)</b>
Method1	180	179	99.45
Method2	180	177	96.70

## References

- [1] Zhang G, Wang H. SURF-based Detection of Copy-Move Forgery in Flat Region, International Journal of Advanced Comput. Technology. 2012;4(17).
- [2] Chihoui T, Bourouis S, Hamrouni K. Copy-move image forgery detection based on SIFT descriptors and SVD-matching. In: Advanced Technologies for Signal and Image Processing (ATSIP), 2014 1st International Conference on. IEEE; 2014. p. 125–9.
- [3] Amerini I, Ballan L, Caldelli R, Del Bimbo A, Del Tongo L, Serra G. Copy-move forgery detection and localization by means of robust clustering with J-Linkage. Signal Process Image Commun. 2013;28(??):659–69.
- [4] Swapnil HK, Gawande A. Copy-Move Attack Forgery Detection by Using SIFT, International Journal of Innovation Technology Engineering IJITEE. 2013;2(??).
- [5] Liu B, Pun C-M. A SIFT and local features based integrated method for copy-move attack detection in digital image. In: Information and Automation (ICIA), 2013 IEEE International Conference on. IEEE; 2013. p. 865–9.
- [6] Bo X, Junwen W, Guangjie L, Yuewei D. Image copy-move forgery detection based on SURF. In: Multimedia Information Networking and Security (MINES), 2010 International Conference on. IEEE; 2010. p. 889–92.
- [7] Chihoui T, Bourouis S, Hamrouni K. Copy-move image forgery detection based on SIFT descriptors and SVD-matching. In: Advanced Technologies for Signal and Image Processing (ATSIP), 2014 1st International Conference on. IEEE; 2014. p. 125–9.
- [8] Kaur A, Sharma R. Copy-move forgery detection using DCT and SIFT. International Journal of Computer Applications, 2013;70(??):30–4.
- [9] Pandey RC, Agrawal R, Singh SK, Shukla K. Passive Copy Move Forgery Detection Using SURF, HOG and SIFT Features. In: Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014. Springer;2015. p. 659–66.
- [10] Kaur A, Sharma R. Copy-move forgery detection using DCT and SIFT. International Journal of Computer Applications. 2013;70(7):30–4.
- [11] M. Zidan, A.-H. Abdel-Aty, M. El-shafei, M. Feraig, Y. El-Abou, H. Eleuch, M. Abdel-Aty, Quantum Classification Algorithm Based on Competitive Learning Neural Network and Entanglement Measure. Appl. Sci., 9(7), 1277, 2019.
- [12] G. Zhang, Neural Networks for Classification: A Survey. IEEE Trans. Syst. Man Cybern. Part C, 30, 451–462, 2000.
- [13] Berardi, V.; Patuwo, B.; Hu, M. A principled approach for building and evaluating neural network classification models. Decis. Support Syst., 38, 233?246, 2004.
- [14] Huang, Y. Advances in Artificial Neural Networks Methodological Development and Application. Algorithms, 2, 973?1007, 2009.
- [15] A. Sagheer, M. Zidan, M. M. Abdelsamea, A Novel Autonomous Perceptron Model for Pattern Classification Applications, Entropy, 21(8), 763, 2019.
- [16] Hashmi MF, Anand V, Keskar AG. A copy-move image forgery detection based on speeded up robust feature transform and Wavelet Transforms. In: Computer and Communication Technology (ICCCT), 2014 International Conference on. IEEE; 2014. p. 147–52.
- [17] Saiqa Khan, Arun Kulkarni (2010),” Robust Method for Detection of Copy-Move Forgery in Digital Images”, International Conference on Signal and Image Processing.
- [18] Diaa M. Uliyan, Hamid A. Jalab, Ainuddin W. Abdul Wahab,”Copy Move Image Forgery Detection Using Hessian and Center Symmetric Local Binary Pattern”,IEEE Conference on Open System, Aug 24-26, 2015.
- [19] Jian Li, Xiaolong Li, Bin Yang, and Xingming Sun, ”Segmentation-Based Image Copy-Move Forgery Detection Scheme”, IEEE Transactions On Information Forensics And Security, Vol. 10, No. 3, March 2015.
- [20] M. Sridevi, C. Mala, And S. Sandeep,”Copy–Move Image Forgery Detection In A Parallel Environment,” 2012.

- [21] Junwen Wang Guangjie Liu Hongyuan Li Yuewei Dai Zhiqian Wang,"Detection of Image Region Duplication Forgery Using Model with Circle Block",International Conference on Multimedia Information Networking and Security,pp.no.26-29,2009
- [22] Z. Mohamadian And A. A. Pouyan, "Detection Of Duplication Forgery In Digital Images In Uniform And Non-Uniform Regions," In Uksim, 2013,Pp. 455-460.
- [23] Gul Muzaffer, Ozge Makul, Beste Ustubioglu, (2016)" Copy Move Forgery Detection Using Gabor Filter and ORB" , International Conference on Image Processing Production and Computer Science pp. 23-29 .
- [24] Pandey RC, Singh SK, Shukla K, Agrawal R. Fast and robust passive copy-move forgery detection using SURF and SIFT image features.In: Industrial and Information Systems (ICIIS), 2014 9th International Conference on. IEEE; 2014. p. 1-6.



#### **S. Devi Mahalakshmi**

received the B.E. degree in Computer Science and Engineering from the Manonmaniam Sundaranar University at Tirunelveli, TamilNadu, India , the M.E. degree in Computer Science and Engineering from the Anna University at Chennai, TamilNadu, India and the Ph.D. degree in Information and Communication Engineering from the Anna University at Chennai, TamilNadu, India. She has over 22 years of teaching and research experience. She is currently an associate professor with the department of computer science and engineering, Mepco Schlenk Engineering College, Sivakasi,(Autonomous), Tamil Nadu, India. She has authored a number of international Journal papers in reputed international journals of computer science and engineering. Her research interests include machine vision and image forensics, medical imaging, IOT and image analysis, in agriculture. She has served on Review committees of various international journals.