IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

COPY-MOVE FORGERY DETECTION USING DUPLICATION DETECTION AND ROBUST DETECTION ALGORITHM

[1]Shuchith M, [2]Dr. Preethi N. Patil

[1]Student, [2]Assistant Professor
[1] Master of Computer Applications,
[1]Rashtreeya Vidyalaya College of Engineering®, Bangalore, India

Abstract: Copy-move is one type of attack to falsify digital images where the perpetrators copy several regions of the image and then place it on different parts of the same image to cover the part of the image that exists in the area. Therefore, a method is needed to detect copy-move attacks to find out the level the authenticity of a digital image. Image data is often deliberately carried out processes such as the addition of noise and blurring so that copy-move attacks are more difficult to recognize, so that the input image preprocessing stage is a filtering process to eliminate noise in the input image. Stages of detection of copy-move attacks can be shortened by not doing the preprocessing stage but using reliable methods for interference such as noise and blur. Therefore, reliable copy-move attack detection methods are needed for various input image variations so there is no need for preprocessing stages on input images. In this a method created from the modification of two methods of copy-move attack detection, an effective duplication detection method, is used on disturbing images and effective detection methods that are used on images that have disturbances such as noise and blur. Modification of the method is considered effective because of the tolerance between the features of the two methods used. When the input image is distraction-free, the duplication detection feature will become dominant, while the input image has disturbances such as noise and blur, the robust detection feature will become dominant.

***Index Terms* - Region Copy-Move, Duplication detection method, Robust detection method, Principal Component Analysis.**

I. INTRODUCTION

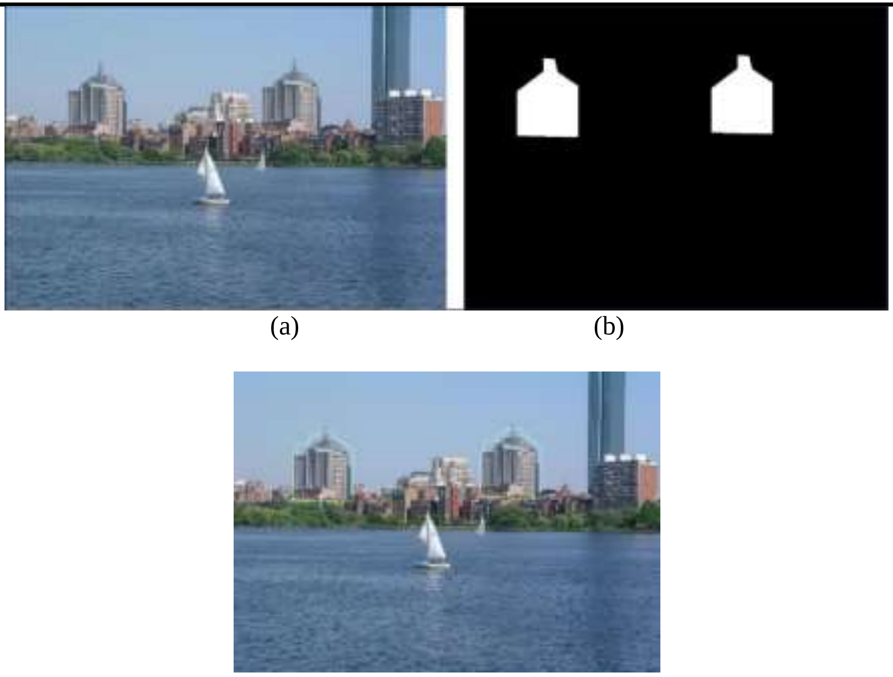
Rapid technological advances make image manipulation much easier. One type of image manipulation is copy-move or duplication of a part of an image to be placed in another location to cover some objects that do not want to be displayed. There have been many cases of fraud involving copy-moves that occurred both in the image in the newspaper and official reports. Not just copy-moves, often the image forgers perform a series of processes after image manipulation which is then called the post region duplication process to make it difficult for others to find evidence of the falsity of the images [1].

Some examples of these processes are blurring, sharpening, JPEG compression and noise addition. There have been studies related to image forgery detection algorithms for various cases such as duplication of an area, color filter interpolation, and re-sampling [8]. There is also a way to detect forgery images by calculating directly on all images or by cutting the image into several parts first. Each of these methods has their respective advantages but has the same weaknesses in the detection of images that have been carried out post region duplication process such as adding noise and blurring operations [3].

Post registration duplication process will change some pixel values on the part of the copy-move, so using an algorithm that only compares individual pixel values is not enough to detect duplicated areas. A journal provides a method for obtaining characteristics of a portion of an image that will not change much even if it is done blurring and sharpening so it is reliable to be used in proving copy-move of images that have been carried out by post region duplication process[6].

Utilizing these properties, a duplication detection algorithm was taken which utilizes PCA to be used as an initial framework and then modified by adding several methods based on the robust detection algorithm [2]. This modification and implementation are expected to produce a copy-detection algorithm move which is faster than the usual brute force algorithm and is also reliable for detecting images that have been carried out in the post region duplication process. Fig. 1 shows the example for a Copy-move forgery and the detection results by the proposed method [5]. The forged image shown in Fig. 1(a) is done by copying a part from the image and pasting it in the same image as shown in the Fig. 1(a) without applying any post processing techniques.

Finally, copy-move forgery detection technique aims at detecting the similar regions in the forged images, by using similarity between the features in those regions. Forgery can also made difficult by doing smoothing the regions to cover up the forgery and making the forgery detection very difficult. Most of many existing detection methods fails to detect the forgery in the smooth non-textured regions. Therefore, it is very important to develop the algorithms which prove the authenticity of forged images [4].



(a) (b)

(c)

Fig 1. Example of a Copy-Move forgery: (a) forged imaged (b) ground truth image (c) detection results

II. Related work

The paper [9], describes a review on IFD approaches are applied for both Copy-Move and spliced images. The survey tries to cover tangled algorithms, and to classify them in classes having the alike approaches to resolve difficulties. the arrangement depends on variations in processing input images transformation before extracting the image features [9]. For the spliced images, groups of detection techniques based on image features.

In this paper [10], an orthogonal wavelet transform based forgery detection method is anticipated. Orthogonal wavelet transform is produced from elementary orthogonal transforms. A Study producing DCTW transform and WW transform from DCT and Walsh orthogonal transforms. The image is separated into overlapping blocks [10]. For individual block, DCTW and WW transforms are implemented. Extraction is done from individual block features using coefficients. These feature vectors are lexicographically sorted, and block matching step is implemented in order to find replicated blocks.

In this paper [11], an efficient robust algorithm is used to detect the forgery. In the first step, the image data is separated into blocks, and DCT is applied to the block thus, the coefficients if DCT represents each block in the image. In the second step the cosine is converted into block which is then represented by a circle and after the previous step the features extraction is done to decrease the dimension. In the final step, the feature is lexicographically sorted, and replicated image blocks is corresponding by a threshold value [11]. This approach shows that the result is not only robust to multiple forgery, but it can also able to detect the blurring or nosing in the image.

In the paper [12], a key point-based image forgery detection method based on a super pixel dividing algorithm and Helmert transformation has been used. The determination of this method is to spot copy-move forgery images and to find forensic info. This procedure comprises the following stages. In the first step, then extraction is done using the key points and by using SIFT algorithm. The matching is done based on by calculating the similarity between key points. In the next step, clustering is done based on the matching pairs and by using the spatial distance and by using Helmert transformation to obtain the forged regions [12]. In the final step, the forged regions are located precisely, and this approach is more vigorous result for scaling and rotation forgeries.

In paper [13] the forgery detection method proposed using the block based and key points this scheme is integrated, In the first step using the adaptive over segmentation algorithm the host image is divided into non overlapping and irregular blocks respectively on host image. After the first step the feature points extraction is done for each block as block features and after the extraction, the extracted block features are matched with each another in the same image and to identify the feature points.[13] To get more accurately, feature points with small pixels are used as feature blocks and it is concatenated with the neighboring blocks.

The paper [14], describes a review on IFD approaches are applied for both Copy-Move and spliced images. The survey tries to cover tangled algorithms, and to classify them in classes having the alike approaches to resolve difficulties. the arrangement depends on variations in processing input images transformation before extracting the image features [14]. For the spliced images, groups of detection techniques based on image features.

III. Proposed methodology

The combination of Duplication Detection and Robust Detection Algorithm is used. The first method runs quickly but is sensitive to low quality images such as those that have a lot of noise. Blurring operations on the image that have been carried out by duplicating attacks can directly threat to the detection process. The second method runs slowly but is reliable on image variations and can recognize the same area despite the blurring process.

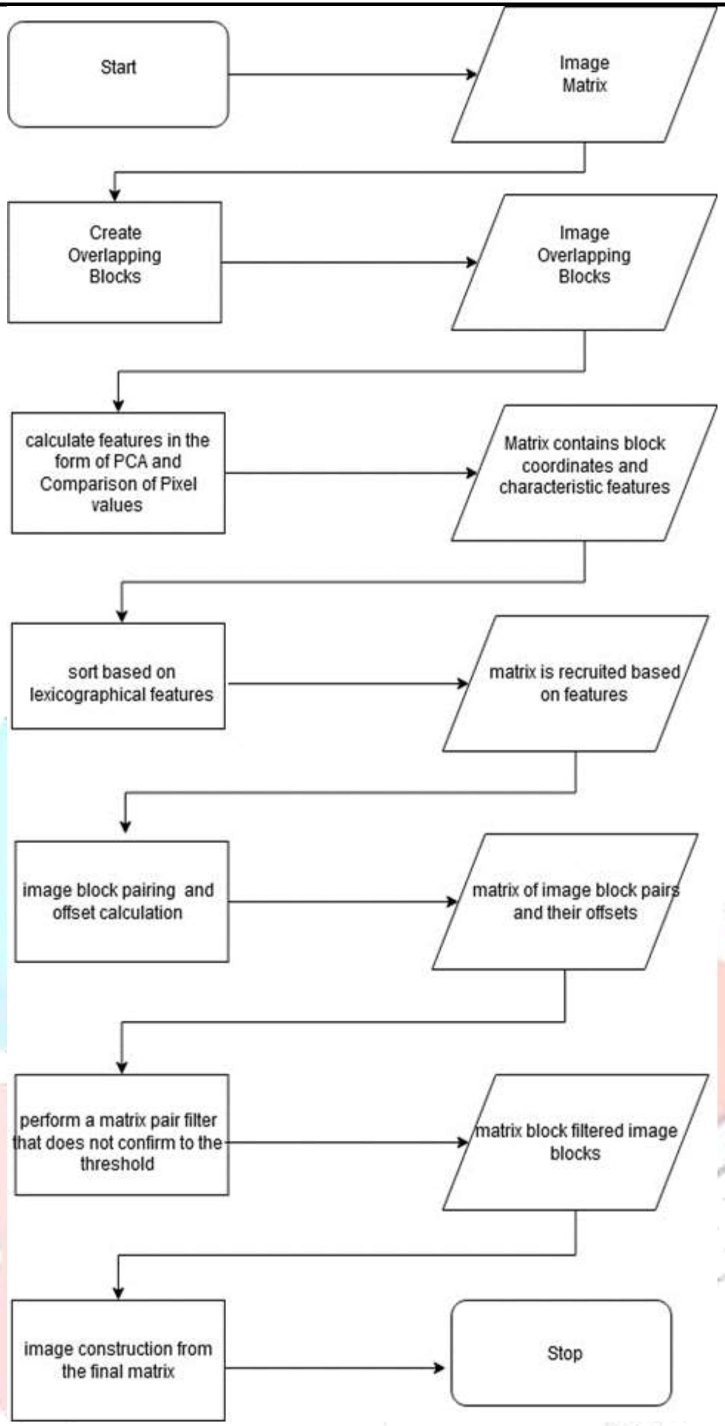

Start
Image Matrix
Create Overlapping Blocks
Image Overlapping Blocks
calculate features in the form of PCA and Comparison of Pixel values
Matrix contains block coordinates and characteristic features
sort based on lexicographical features
matrix is recruited based on features
image block pairing and offset calculation
matrix of image block pairs and their offsets
perform a matrix pair filter that does not confirm to the threshold
matrix block filtered image blocks
image construction from the final matrix
Stop

Fig 2. Modification of Robust Detection Algorithm and Duplication Detection Algorithm

Step 1: The given input image is divided into size M x N into image blocks with a size of L x L which is relatively small and overlapping one another. The image block is then called the overlapping block. The number of overlapping blocks in an image, which is then named the variable N_b can be calculated using Equation 3.1.

$$N_b = \frac{(M-L+1)}{i} \times \frac{(N-L+1)}{j} \qquad (3.1)$$

Step 2: Feature extraction is performed to obtain the features of each image block. At this stage there are two processes for calculating features. First is PCA, and second is the rule of comparing pixel values.
Step 3: Prepare the array of inputs $x^{\rightarrow}$. This array contains pixel values of image blocks formed by a vector and has a number of N_b elements.
Step 4: For grayscale images, the array is an array of size M x N which contains pixel value in the corresponding coordinates which then form vectors so that they form a single line.
Step 5: For color imagery, build a 3b pixel by pixel block consisting of red, green and blue pixels, then do the PCA process [7].
Step 6: Determine the value N_t which is the number of dimensions to be taken. This stage has several steps namely calculating the covariance matrix of the array $x^{\rightarrow}$ with Equation 3.2, then calculating the eigenvector $ej^{\rightarrow}$ and eigenvalue λj so that it meets Equation 3.3.

$$C = \sum_{i=1}^{Nb} \vec{x_i}\ \vec{x_i}^{\mathrm{T}} \qquad (3.2)$$

$$C\vec{e_j} = \lambda_j \vec{e_j} \qquad (3.3)$$

Step 7: Using eigenvector $\vec{e}$, the principal component can be determined by forming a new matrix of dimensions for each image block $\vec{xi}$ using equation 3.4, with j = 1 ..., b and $\lambda 1 \geq \lambda 2 \geq \cdots \geq \lambda b$, where aj = $\vec{xi}^{T}\vec{ej}$ and $\vec{ai}$= (a1 ... ab) are principal component and this will be used as the new data representation.

$$\vec{x_i} = \sum_{j=1}^{b} a_j \vec{e_j} \tag{3.4}$$

Step 8: Save the coordinate image data block together with the principal component belonging to the matrix $\vec{a}$ into the matrix $\vec{s}$. The output of the coordinate image block and PCA data describes that the end of the first stage of the first process.
Step 9: Calculation of the ratio of pixel values. If the input image has a color space other than grayscale, change the color colors of the image to RGB. Calculate the first three characteristics (c1, c2, c3), where c1 is the total average of number of pixels in red pixels, c2 is the total average of number of pixels in green pixels, c3 is the total average of number of pixels in blue pixels. If the input image contains color space grayscale, then the value of c1, c2, c3 are assigned to zero.
Step 10: Change the color block of the image block to Y channel by replacing the pixel value with each of with the new value obtained from Equation 3.5, where R, G, and B are the red, green and blue pixel values of a pixel.

$$Y = 0.299\ R + 0.587G + 0.114B \tag{3.5}$$

Segmentation of the image into four kinds of patterns as shown in Figure 3 which divides the image blocks into two equal parts.

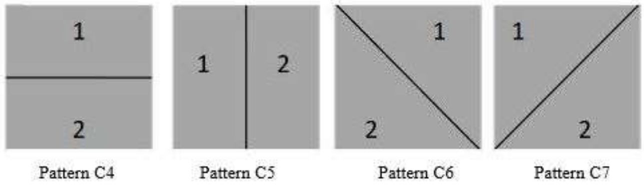


Fig 3. Dividing images into four Patterns

Step 11: A container $\vec{s}$ contains a collection of data pairs in the form of coordinates of the image block represented by the coordinates of the upper left end of the image block, along with the results of the PCA and the comparison of pixel value which have been obtained.

$$Ci = sum(part1(i))/sum(part1(i)+part2(i)) \tag{3.6}$$

Step 12: The container $\vec{s}$ is then sorted using the lexicographical sorting method based on the PCA value and the pixel comparison feature on each image block. After sorting, the image blocks with the principal component and the comparative features of the same or similar pixel value which will be located close together.
Step 13: Create a new matrix $\vec{t}$ and fill it with the coordinate pairs of image blocks (xi, yi) and (xj, yj) only if | i − j | < Nn, where i and j are the index blocks of images in the container $\vec{s}$ and Nn are the maximum limits neighbor distance that is calculated. In the fifth stage, calculate the offset from each element of the matrix $\vec{t}$ called Equation 3.7.

$$Offset = (xi – xj, yi – yj) \tag{3.7}$$

Step 14: The sixth step remove all coordinate pairs in the matrix $\vec{t}$ which has an offset frequency less than Nf.

$$N_d = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \tag{3.8}$$

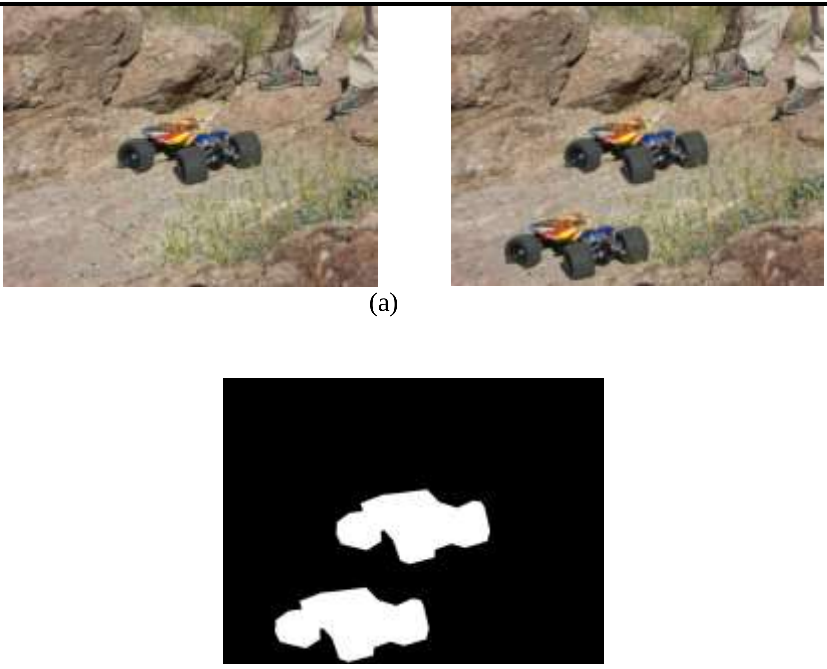
Step 15: The seventh stage discard all coordinate pairs in the matrix $\vec{t}$ which has an offset value less than N_d, where the offset value is calculated by Equation 3.8.
Step 16: Finally, create a ground truth image by creating a binary image (black and white) with a standard value of 0, and giving a value of 1 at each location of the remaining image block pairs. From the ground truth image, duplicate the input image and give a colored line to each edge of the white area using the ground truth to get the detected image.

IV. Challenges

- How to detect copy-move attacks on images that have been carried out post region duplication processing?
- Is the method of modification of duplication detection and robust detection algorithms can be used to detect copy-move attacks on images that have been the post region duplication processing process is carried out?
- How do you modify the duplication detection and robust detection algorithm to be reliable and adaptable to the type of input image?

V. Results

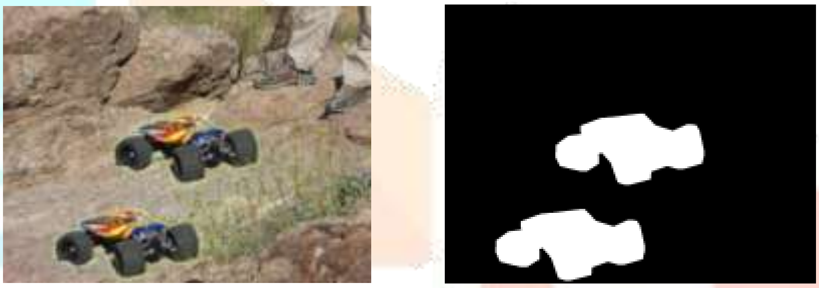
The Fig 4(a) is the original image, Fig 4(b) is the Forged image, Fig 4(c) is the Ground truth image provide from the public dataset. Fig 5(a) is the input data will be processed using the duplication detection, robust detection, and modification methods. The results of the copy-move attack detection process in each of these methods are two input imagery images with the allegedly falsified area marked by a colored line and the resulting image detection by default is black while the allegedly duplicated area is colored white, shown in Fig 6(a), Fig 6(b) and Fig 6(c). To measure accuracy, another program is created which functions to calculate the similarity of output to ground truth using the mean squared error and similarity methods.



(a) (b)

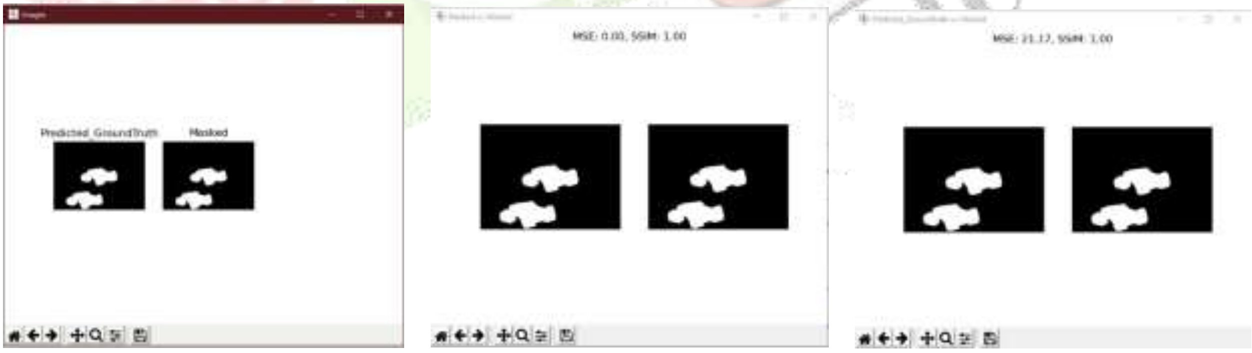
(c)

Fig 4. (a) Example of authentic image input data, (b) Example of image input data affected by a copy-move attack, (c) Example of ground truth data from image detection results affected by copy-move attacks



(a) (b)

Fig 5. (a) Example of the resulting image that gives color lines to areas suspected of being forged, (b) Example of the output image that shows the results of counterfeiting detection



MSE: 0.00, SSIM: 1.00

MSE: 21.17, SSIM: 1.00

(a) (b) (c)

Fig 6. (a) Example of the image of Counterfeiting detection and Ground truth, (b) Example of the image comparing Ground truth vs Ground truth, (c) Example of the image comparing Counterfeiting detection and Ground truth

VI. Conclusion

The implementation of the duplication detection method can be used as a method for detecting and analyzing copy-move attacks on images that are not done in the post region duplication process. Modification of the method in the form of using offset values that are not carried out absolute operations can increase accuracy. The implementation of the robust detection method can be used as a method for detecting and analyzing copy-move attacks on images carried out by the post region duplication process. Modification of the method in the form of replacing the use of the histogram to use a minimum threshold can improve the ability of the method to detect copy-move attacks carried out on more than one pair of regions. The three methods used, namely duplication detection, robust detection, and robust-duplication detection cannot detect overlapping copy-move attack areas. The greater the jump that occurs in making overlapping blocks, the less time it takes for the method to detect the image, with a decreased accuracy trade-off.

REFERENCES

[1] Maind, Rohini. A., Alka Khade and D. K. Chitre. "Image Copy Move Forgery Detection using Block Representing Method." (2014).

[2] T. Chihaoui, S. Bourouis and K. Hamrouni, "Copy-move image forgery detection based on SIFT descriptors and SVD-matching," 2014 1st International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), Sousse, 2014, pp. 125-129.

[3] S. Sharma and U. Ghanekar, "A Rotationally Invariant Texture Descriptor to Detect Copy Move Forgery in Medical Images," 2015 IEEE International Conference on Computational Intelligence & Communication Technology, Ghaziabad, 2015, pp. 795-798.

[4] Qureshi, M. A., & Deriche, M. (2015). A bibliography of pixel-based blind image forgery detection techniques. Signal Processing: Image Communication, 39, 46–74.

[5] J-C. Lee, Copy-Move Image Forgery Detection Based on Gabor Magnitude, J. Vis.Commun. Image R. (2015).

[6] C. Pun, X. Yuan and X. Bi, "Image Forgery Detection Using Adaptive Over segmentation and Feature Point Matching," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 8, pp. 1705-1716, Aug. 2015.

[7] J. Li, X. Li, B. Yang and X. Sun, "Segmentation-Based Image Copy-Move Forgery Detection Scheme," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 507-518, March 2015.

[8] Tu K. Huynh, Thuong Le-Tien, Khoa V. Huynh and Sy C. Nguyen, "A Survey on Image Forgery Detection Techniques", The 2015 IEEE RIVF International Conference on Computing & Communication Technologies Research Innovation and Vision for Future (RIVF), pp. 71-76, 25-28 Jan. 2015.

[9] C. Lee et al., Detection of copy–move image forgery using histogram of orientated gradients, Inform.Sci. (2015).

[10] Yu, L., Han, Q. & Niu, X. Feature point-based copy-move forgery detection: covering the non-textured areas. Multimed Tools Appl 75, 1159–1176 (2016).

[11] M. Emam, 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.

[12] M. A. Elaskily, H. K. Aslan, O. A. Elshakankiry, O. S. Faragallah, F. E. A. El-Samie and M. M. Dessouky, "Comparative study of copy-move forgery detection techniques," 2017 Intl Conf on Advanced Control Circuits Systems (ACCS) Systems & 2017 Intl Conf on New Paradigms in Electronics & Information Technology (PEIT), Alexandria, 2017, pp. 193-203.

[13] R. Dixit, R. Naskar and A. Sahoo, "Copy-move forgery detection exploiting statistical image features, "2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, 2017, pp. 2277-2281.

[14] Kuznetsov, A., & Myasnikov, V. (2017). A new copy-move forgery detection algorithm using image preprocessing procedure. Procedia Engineering, 201, 436–444.

[15] Wang, X., Liu, Y., Xu, H. et al. Robust copy–move forgery detection using quaternion exponent moments. Pattern Anal Applic 21, 451–467 (2018).