DETECTION OF COPY MOVE FORGERY IN DIGITAL IMAGES

Gurpreet Kaur[1*], Dr. R.K. Bathla[2#]
[1*]Research Scholar: Department of Computer Science, Desh Bhagat University, Mandi Gobindgarh, India,
[2#] Professor: Department of Computer Science, Desh Bhagat University, Mandi Gobindgarh, India.

ABSTRACT: One of the most common method of digital image forgery is copy move forgery.It means to embed a duplicacy. In other words, copy move forgery is that where some image location is copied and pasted to different location of the same image.To hide the forgery,post processing is applied.In this paper,an effective method for copy move foegery is proposed.For this, block based feature extraction and matching process is used. At first edge detection is carried out to get the high entropy pixels in the image so that matching process is carried out only for high entropy pixel blocks. Then feature extraction is carried out by converting image into overlapped blocks and mean and DCT features are extracted. Then mean values are put into a matrix and corresponding blocks are noted. Then mean value matrix is sorted in order to match the blocks with similar mean values. In matching process, variance of DCT features is used for similarity measure and forgery detection. Experimental results show that proposed method has high accuracy of forgery detection along with least computation time.

Keywords—Copy Move Forgery, Block Based Forgery Detection, Mean, Variance, DCT etc.

I. INTRODUCTION

We are living in the era of digital eolution,where it is very easy to access,process and share information.With the increased use of technology,it is very easy to bring changes in the original image.But it is very difficult to detect forgery with naked eyes.Due to this problem, researchers suggest some methods to examine the originalty of digital images.In this paper we discover the problem of indentifying the type of digital image forgery---copy move forgery.Copy move forgery is one of the most popular image forgery technique. The image forgery detection is explored to passive and active methods [3].Image Forgery is of two types: copy-move forgery and splicing forgery [4]. In copy-move forgery, portions of one image are copied and then pasted into the image itself, whereas in splicing forgery; portions of one or more images are copied and then pasted into a different image. Recognition of copy-move forgery has been extensively investigated [4]. Established approaches for copy-move forgery detection can be regarded as keypoint-based and block-based methods. Keypoint-based methods embrace scanning of the entire image with the target of verdict points of attention (for example, point with high entropy). Those opinions are then examined to select only point with the identical possessions and distinguish analogous zones in the image. Various prevalent instances of keypoint-based methods are SIFT (Scale-invariant feature transform) [5] and SURF (Speeded Up Robust Features) [6]. Block-based approaches comprise separating an image into insignificant overlying blocks as a leading phase of the process. A set of features is then intended for each definite block, and those features are castoff for detection of analogous blocks in the image. Diverse sets of features, for instance DCT (Discrete Cosine Transform) [4] / DWT (Discrete Wavelet Transform) [7] factors, Zernike moments [9] or PCA (Principal Component Analysis) [8], have been projected for practice in block-based methods.

- **Block-Based Method for CMFD**

In general all block-based copy move forgery detection approaches track analogous phases:

Firstly, we divide image into blocks of size
16 _ 16 and each of these blocks is represented with the 9 characteristics. These characteristics are as follows. First, the average value of the intensity of the block is calculated. Then, each block division is divided into to four identical subblocks and the remaining 8 characteristics concerning the relationship between block and subblock. Four characteristics mark the ratio of the average intensity of each of the washers with the block, and the remaining four indicate the
difference of the average intensity of each subblock and block of which they are part. This can be formally
written as:

$$f_i = \begin{cases} f_i = Ave(B) & \text{if } i = 1, \\ Ave(S_{i-1})/(4Ave(B) + \varepsilon_1) & \text{if } 2 \leq i \leq 5, \\ f_i = Ave(S_{i-5}) - Ave(B) & \text{if } 6 \leq i \leq 9.| \end{cases}$$

Thus obtained characteristics are normalized to
the rank of 0 to 255. This is done by the following
formula:

$$x_i = \begin{cases} \lfloor f_i \rfloor & \text{if } i = 1, \\ \lfloor 255 \times f_i \rfloor & \text{if } 2 \leq i \leq 5, \\ \lfloor 255 \times \frac{f_i - m_2}{m_1 - m_2 + \varepsilon_2} \rfloor & \text{if } 6 \leq i \leq 9, \end{cases}$$

where $m_1 = \max f_i,\ 6 \leq i \leq 9$ and $m_2 = \min f_i,\ 6 \leq i \leq 9$

In order to increase the chance of image protection from different modifications, it is easier to manipulate the image when is divided into blocks of size 16x16 using the vector with nine dimensions, which can be moved as a block, which consists of four blocks of equal size Sa, Sb, Sc, Sd. So f1 has an average intensity of the block B, and f2, f3, f4, f5 are intensities blocks of Sa, Sb, Sc, Sd. These 9 values sometimes contain duplicate information, they have a greater chance to prevent changes to the image, such as for example is compression. Rotating is discovered
by leveraging image with its rotated versions. The examples are based on 270 and 180 degrees. If this is how we are working we can detect fraud at any angle. To find a copied image, we combine the three versions of the image that are rotated with the original image and with these combined images the fraud is found.

II. PROPOSED SYSTEM

In this work, block based feature extraction and matching process is used. At first edge detection is carried out to get the high entropy pixels in the image so that matching process is carried out only for high entropy pixel blocks. Then feature extraction is carried out by converting image into overlapped blocks and mean and DCT features are extracted. Then mean values are put into a matrix and corresponding blocks are noted. Then mean value matrix is sorted in order to match the blocks with similar mean values. In matching process, variance of DCT features is used for similarity measure and forgery detection. The flowchart of the methodology has been shown in Figure 1.

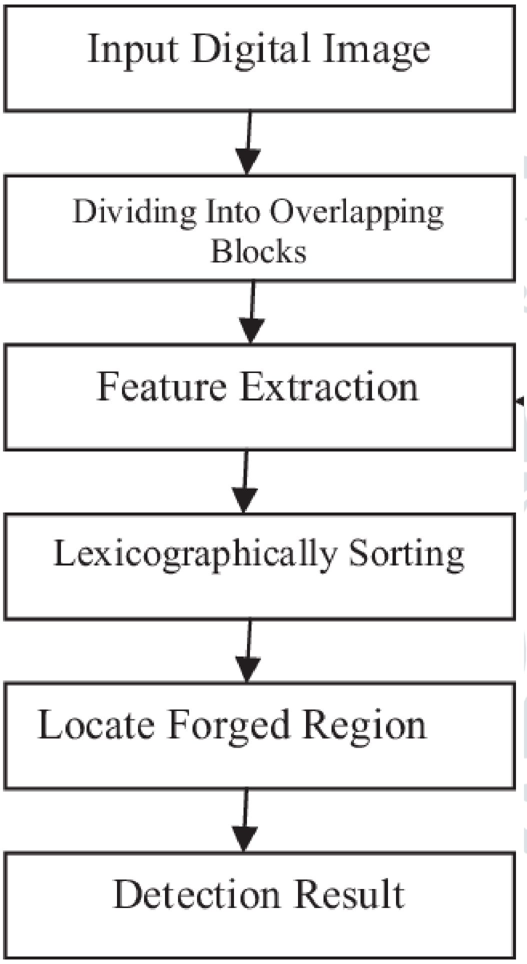


Figure 1: Flowchart of the proposed method

Steps in the proposed algorithm are as follows :

(1) Initially we take the forged image of size $R_{rows} \times C_{cols}$ pixels (say) as an input. If the image is RGB format, we convert it into grayscale using to following Eqn.:

Img$_{gray}$=0.299*Red channel+0.587*Green channel+0.114*Blue channel

(1)

(2) Applied Gabor filter twice to enhance the edge pixels in the image by taking grayscale image and its complement image together and merge the output from them and then sobel filter is applied in horizontal and vertical direction to get the improved edge image to which further thresholding is applied to get binary image.

(3) Overlapping blocks of size $X \times X$ pixels has been obtained from the grayscale image, such that total size of obtained blocks is $\left(R_{rows} - X + 1\right) \times \left(C_{cols} - X + 1\right)$. The mean value sequence $M_1,\ M_2\ \ldots M_{((W/2-P+1)\times(H/2-P+1))}$ is calculated from the corresponding blocks $B_1,\ B_2, \ldots\ B_{(R_{rows}-X+1)\times(C_{cols}-X+1)}$, as:

$$M_i = \frac{1}{X \times X} \sum_{j=0}^{X \times X} x_{ij} \qquad (2)$$

where M_i is the mean of pixel intensity of block B_i. The mean values are stored into a matrix, say A which is sorted in ascending order.

(4) Evolution of DCT features for the overlapping blocks.

(5) For calculation of similarity between blocks, we measure the following Euclidean distance:

$$D\left(x,\ y\right)' = \left(\sum_{i-1}^{(\mathrm{R}_{rows}-X+1)} \left(A_{xi} - A_{yi}\right)^2 \right)^{1/2}$$

(3)

where $D\left(x,\ y\right)$ is the Euclidean distance between a pair of rows of $A, A_x\ and\ A_y$, where $A_x = (A_{x1},\ A_{x2}, \ldots A_{x(M_{rows}-X+1\ )}$ and $A_y = \left(A_{y1},\ A_{y2}, \ldots A_{y(C_{cols}-X+1)}\right)$. Similarity check has been applied to only those pixels which come as edges in the soble edge binary image. It reduces the computation time as only high entropy pixels come as edge pixels.

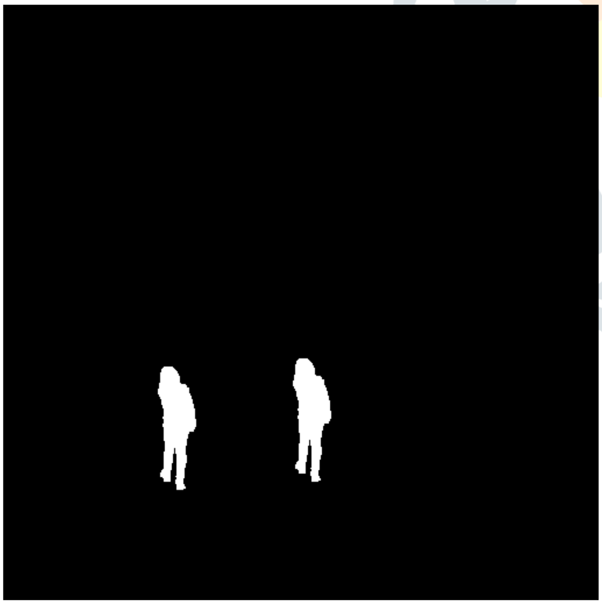
(6) The block pairs for which $D(x, y) < T_s$, (where T_s is an empirically selected similarity threshold), are possibilities to be forged regions.

(7) For the selected edge pixel block check the similarity based on variance value of DCT features; Two block-pairs which has similar variance values, mark them as forged edge pixels.

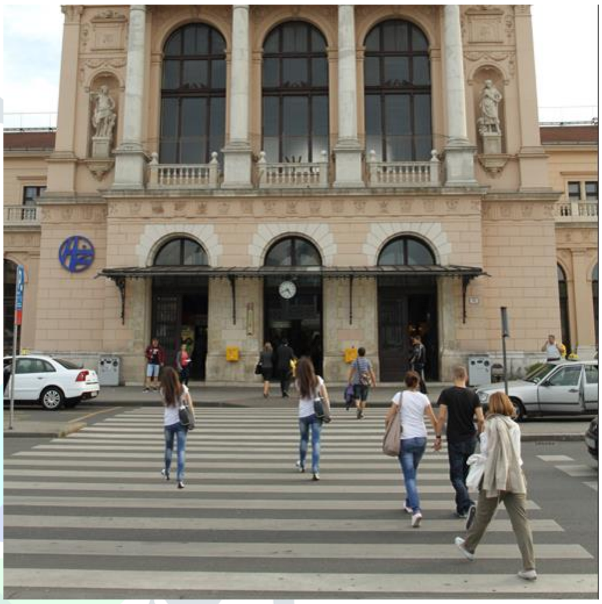
(8) As this produced only edge pixels in the copy move rotated area, morphological operations i.e. dilation and erosion is applied to the output, to which further similarity matching based on variance difference of DCT value is applied which results in whole forgery area detected in the image. The method is efficient and provides good results in Copy-move forgery detection.

III. EXPERIMENTAL RESULTS

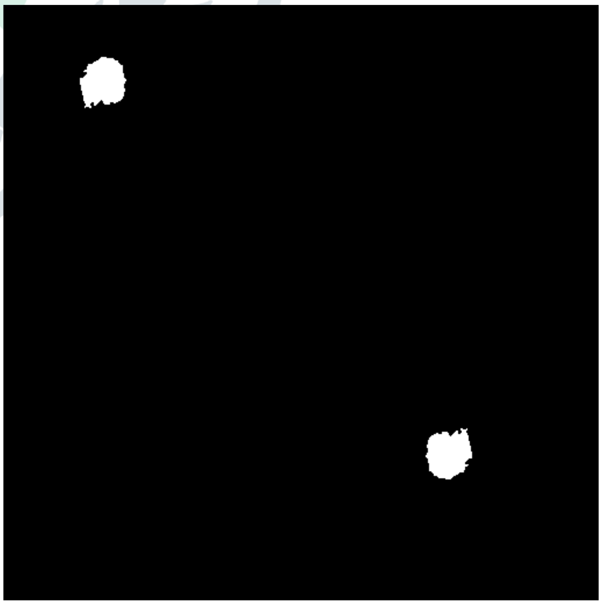
In this paper we used the database for a copymoved forgery detection proposed in [8]. The dataset consists of 260 forged image sets. Every image set includes forged image, two masks and original image. Images are grouped in 5 categories according to applied manipulation: translation, rotation, scaling, combination and distortion. Also, post-processing methods, such as JPEG compression, blurring, noise adding, color reduction etc., are applied at all forged and original images. Examples of dataset are shown in Fig. 2.



(a)



(b)



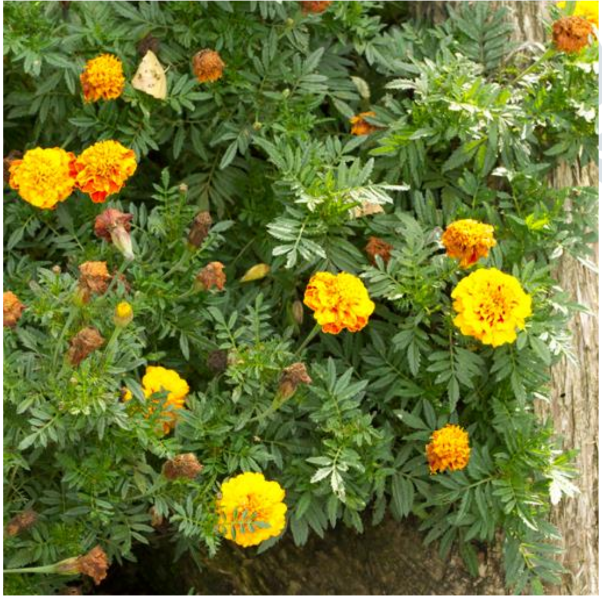
(c)

(d)

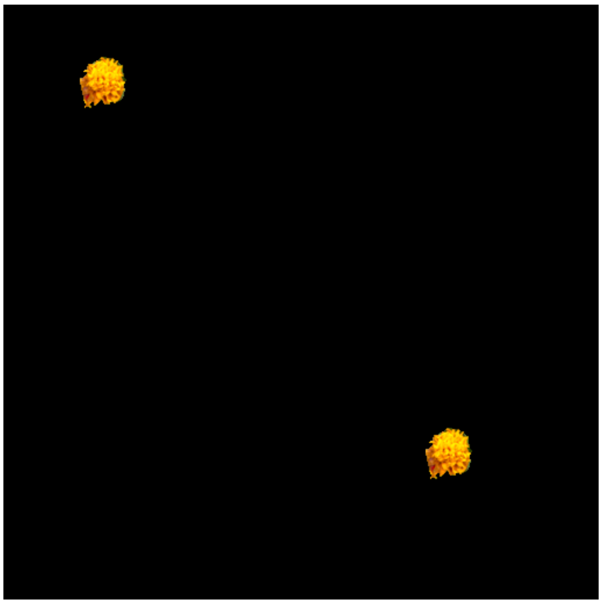
Figure 2: Example of dataset

In Fig. 3, Fig. 4 and Fig. 5 the result of our proposed algorithm are shown. Fig. 3(a) is a picture of nature where the flower is copied. Copied parts are shown in Fig. 3(b). Our algorithm detect copied figures as it can been seen in Fig 3(c). Proposed algorithm was able to recognize copied regions. Fig.4 represents second example where the car is copied.

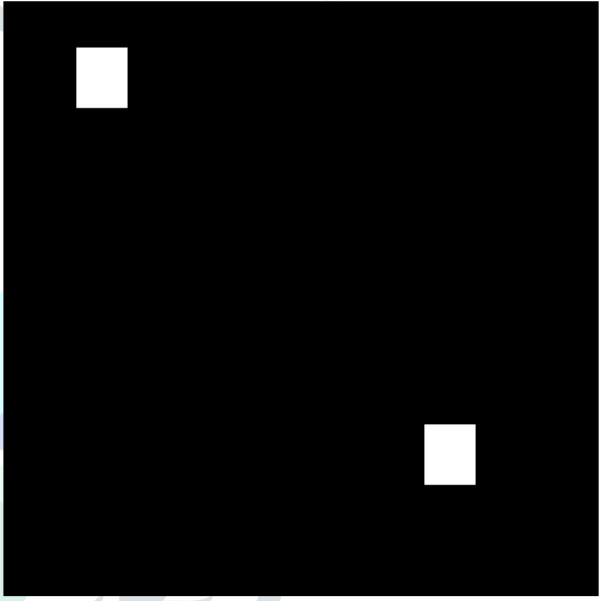
Similar to Fig. 3, Fig. 4(a) is an image that contain copy-move forgery, while in Fig. 4(b) copied regions are shown. Recognition of proposed algorithm is represented in Fig. 4(c). In this case our proposed algorithm was also showed as good. The third example shows the copied pigeon and it is presented in Fig. 5. It can been seen that our proposed algorithm successfully detects image manipulation.



(a)



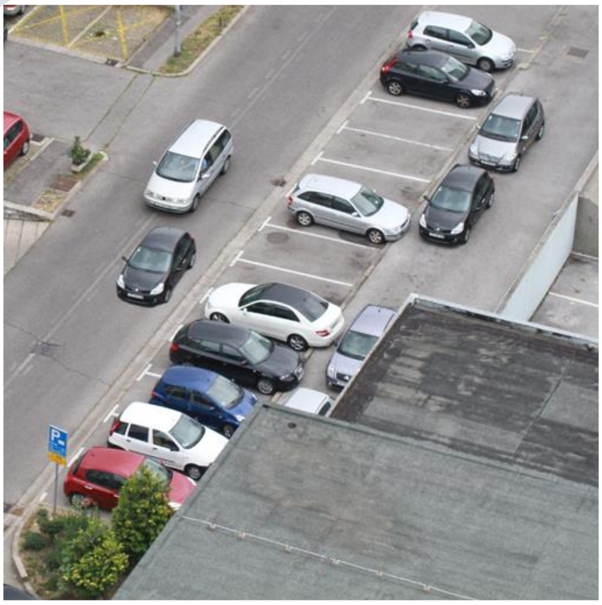
(b)



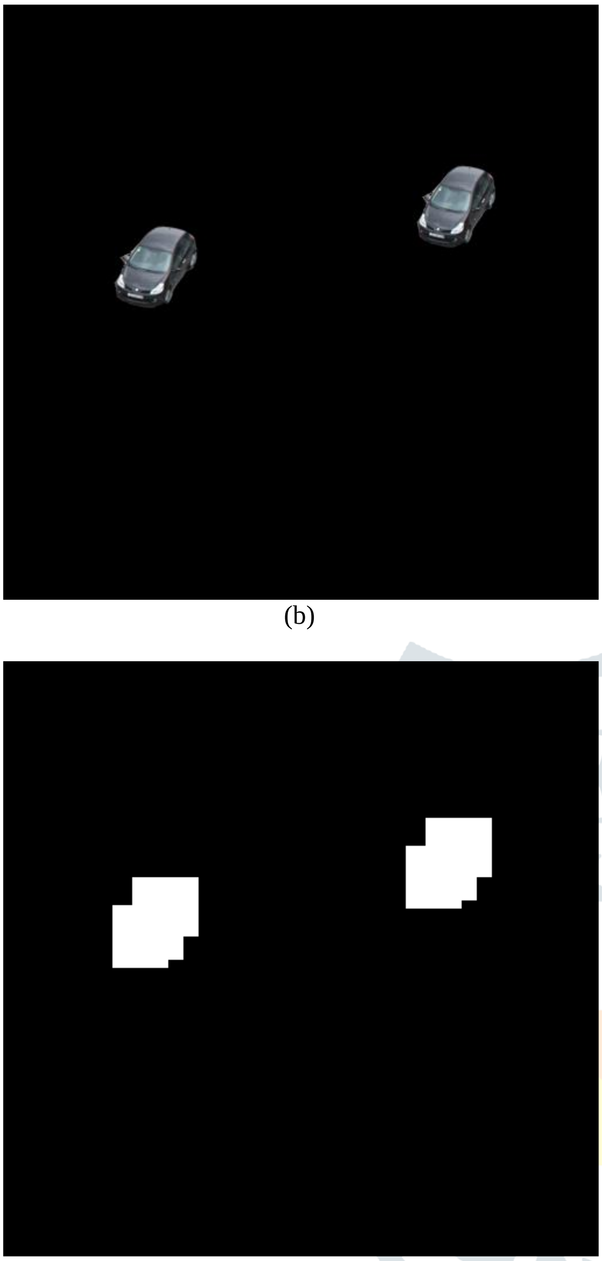
(c)

Figure 3: Experimental results (a) Original, (b) Mask, (c) Recognized regions

FIGURE 3



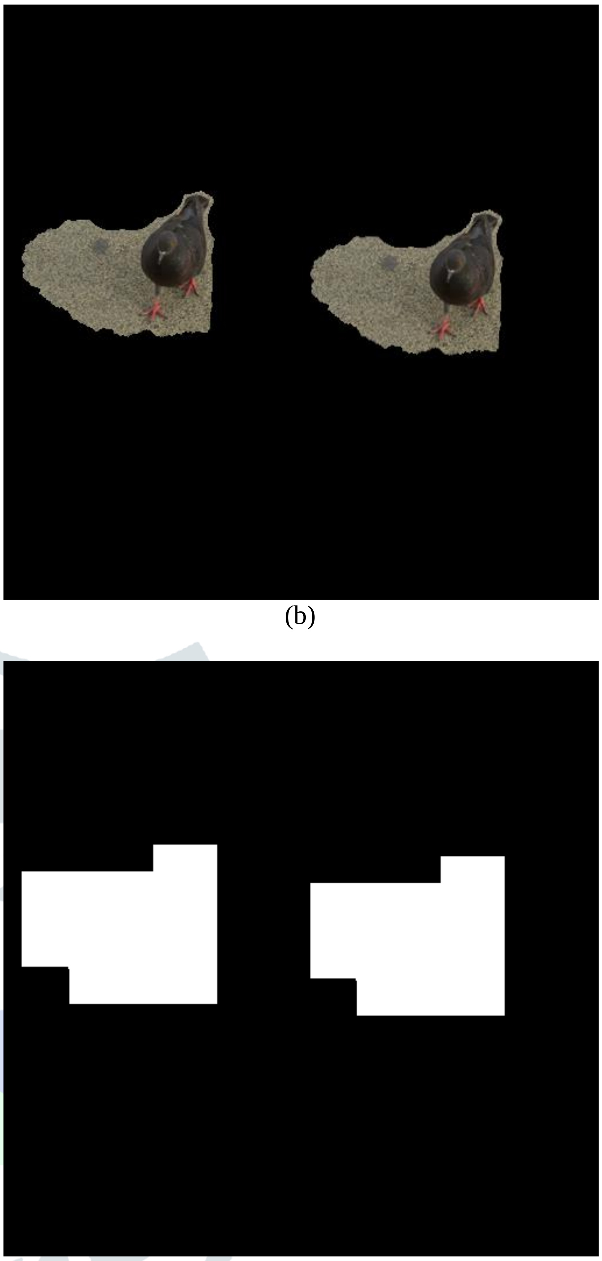
(a)



(b)

(c)

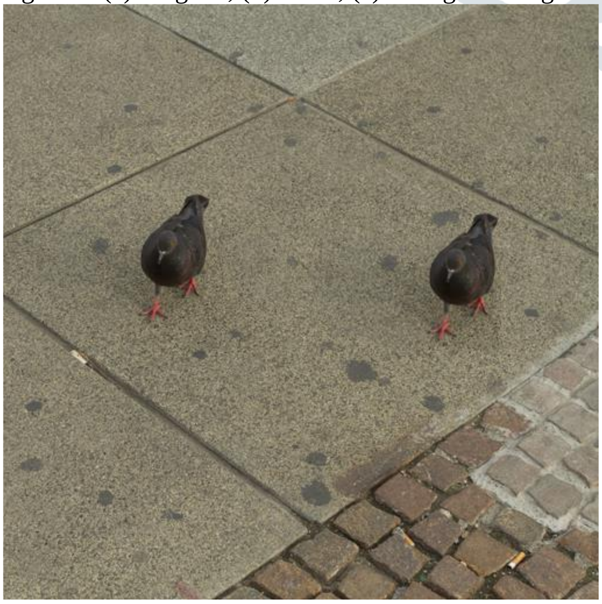
Figure 4: (a) Original, (b) Mask, (c) Recognized regions



(b)

(c)

Figure 5: (a) Original, (b) Mask, (c) Recognized regions



(a)

IV. CONCLUSION

Proposed method was tested on standard benchmark images from [8]. In all cases it successfully detected copy-move forgery, including cases with rotationand compression. In this paper, an efficient block-based method is presented for CMFD. First edge enhancement and edge detection is used to generate a binary image containing edge and non-edge areas, Purpose of edge detection is to reduce the computation time of the algorithm as most of the existed CCMFD algorithms have large computation time. It enables to match only those blocks which come as edge pixel blocks in binary image. Secondly mean and DCT features are used in which mean values of all the overlapped blocks are calculated and sorted and then similarity matching is carried out for those blocks which have similar mean values. Forged areas are marked for those blocks which have similar variance values of the DCT features. Experimental results show high accuracy of forgery detection. Proposed method can amend to include rotation invariant forgery detection as it fails for the rotated copy move blocks.

REFERENCES

[1] R.Singh, A. Oberoi, and N. Goel, “Copy move forgery detection on digital images,” International Journal of Computer Applications, vol. 98, no. 9, pp. 17–22, 2014.

[2] J. Fridrich, D. Soukal, and J. Lukáš, “Detection of copy-move forgery in digital images,” in Proceedings of Digital Forensic Research Workshop, Cleveland, Ohio, USA, August 2003.

[3] Osamah MAQ, KhooBE (2013) Passive detection of copy-move forgery in digital images: state-of-the-art. Forensic Science International, 231:284-295.

[4] FridrichJ, SoukalD, LukasJ (2003) Detection of copy-move forgery in digital images, Proceedings of Digital Forensic Research Workshop, 3:55-61.

[5] AmeriniI,BallanL,CaldelliR, BimboAD and SerraG (2011) A SIFT-based forensic method for copy-move attack detection and transformation recovery. IEEE Transactions on Information Forensics and Security, 6:1099–1110

[6] ShivakumarBL,and BabooS (2011) Detection of region duplication forgery in digital images using surf. International Journal of Computer Science Issues, 8:199–205

[7] BasharM, NodaK, OhnishiN,and MoriK (2010) Exploring duplicated regions in natural images. IEEE Transactions on Image Processing

[8] D. Tralic, I. Zupancic, S. Grgic, and M. Grgic,
“CoMoFoD - new database for copy-move
forgery detection,” in 55th International Symposium

ELMAR, pp. 49–54, Sept 2013.

[9] RyuSJ, LeeMJ and Lee,HK (2010) Detection of copy-rotate-move forgery using zernike moments. International Workshop on Information Hiding: 51–65

[10] WangJ, LiuG, LiH, DaiY and WangZ (2009) Detection of image region duplication forgery using model with circle blocks. International Conference on Multimedia Information Networking and Security: 25-29

[11] ZhengN, WangY and MingX(2013) A LBP-Based Method for Detecting Copy-Move Forgery with Rotation. Multimedia and Ubiquitous Engineering: 261-267

[12] PandeyRC,AgrawalR, SinghSK andShuklaKK (2014) Passive Copy Move Forgery Detection Using SURF, HOG and SIFT Features. Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA): 659-666

[13] YuL, HanQ,andNiuX (2016) Feature point-based copy-move forgery detection: covering the non-textured areas. Multimedia Tools and Applications, 75:1159–1176

[14] EmamM, HanQ,andNiuX (2016) PCET based copy-move forgery detection in images under geometric transforms. Multimedia Tools and Applications, 75:11513–11527

[15] M. F. Hashmi, A. R. Hambarde, and A. G. Keskar, “Copy move forgery detection using DWT and SIFT features,” in 13th International Conference on Intellient Systems Design and Applications, pp. 188–193, IEEE, 2013.

[16] H.-J. Lin, C.-W. Wang, Y.-T. Kao, et al., “Fast copy-move forgery detection,” WSEAS Transactions on Signal Processing, vol. 5, no. 5, pp. 188–197, 2009.