Rotation Invariant Forgery Detection using LBP Variants

Ms. Gurpreet Kaur[#1], Dr. Rajan Manro
ResearchScholar(Assistant Professor),Assosicate Professor
Department of Computer Science,Desh Bhagat University,Mandi Gobindgarh,India
Department of Computer Science,Desh Bhagat University,Mandi Gobindgarh,India

Abstract

Digital Forensics is anoutlet of forensic science which is connected to cyber-crime. Mostly it includes the detection, recovery and investigation of digital devices. As we now in today's world, Digital images and videos play most important role in digital forensics because they are the majorindicator of any crime scene. So the reliability of the image is important. These images can be easily manipulated and edited with the help of image processing tools. Under this, Copy-move Forgery is the most basic form of cyber-attack on digital images. In Copy-move forgery, particular amount of image (region) itself is copied and pasted into another fragmentof the same image. The idea behind this type of attack is to "add" or "delete" some objects from the image to break the faithfulness of the image and befool the viewer. This type of attack is more dominant in images having same texture or patterns, for e.g. sand, grass, water etc. In some cases when the copied region is processed before pasted i.e. some geometric transformations like rotation, scaling is applied on the pasted region. In such cases, It is not possible for human eyes to detect such kind of forgeries. When forgery is done in this way then techniques like block matching, key points are also unable to detect forgery. Soin thispaper, we explore some rotation invariant methods which are able to detect these kind of forgeries which include geometric transformations.

Keywords - *Digital Forensics, Keyword Based, Gabor Filter,ZM, PZM*

I.INTRODUCTION

We are living in an era of digital revolution which made it very easy to access, process, and share information. With the increased growth of technology, software like Photoshop, Corel Draw, and others, it is becoming very difficult to discriminate between an authentic picture and its manipulated or doctored version. Image forgery is becoming indeed a challenge for individuals as well as for institutions. The basic concept of image forgery is the digital manipulation of pictures with the aim of distorting some information in these images. The images in digital format could be manipulated via forgery that conveys false information without any trait of evidence. A number of available software is dedicated to aid in the conventional approach of forgery, i.e. copy-move-rotate (CMR).

The **forgery** is defined as "The creation of duplicitous copy or imitation of a document, signature, banknote or a work of art". In the domain of digital images, the forgery is the state of art classified in **two models additive approach and subtractive approach** based on the content of the original image. The additive approach copies a segment of random image (or same image) and mixes it with the original image to enhance original information. The subtractive approach clips a part of information from the original image. Subtractive forging of Joseph and Nikolai Yezhov (a) Original image (left) (b) Forged image (Right) (Math & Tripathi, 2011).

Subtractive forging of Joseph and Nikolai Yezhov (a) Original image (left) (b) Forged image (Right) (Math & Tripathi, 2011).

Fig.-1:Subractive Approach of Image Forgery

II.GENERAL FRAMEWORK OF FORGERY DETECTION

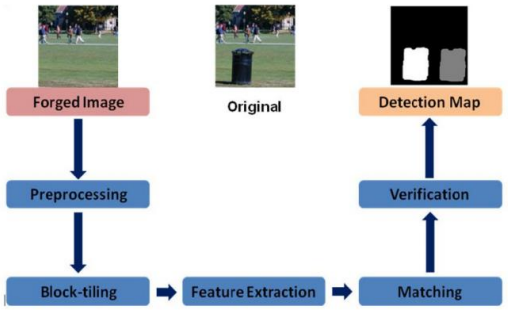

Fig.-2: Framework Of Forgery

III.CLASSIFICATION OF IMAGE FORGERY TECHNIQUES

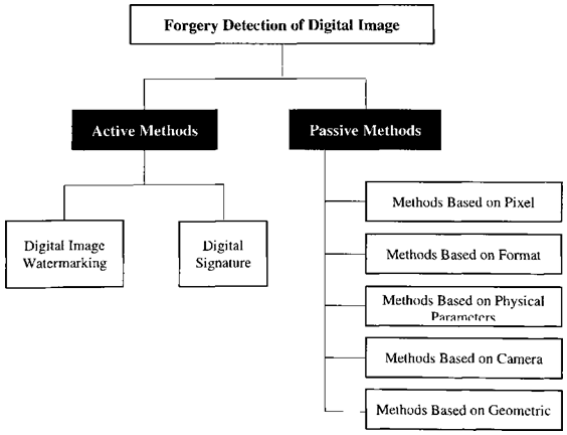

Fig.3: Forgery Detection Methods

A. Active Methods

Active Methods are those methods in which Information is hidden inside the digital image. It is done at the time of Data Acquisition or before disseminated to the public. Here Embedded Information is used to detect the modifications of image. Inspite of this, Active techniques have certain limitations because they require human intervention or specially equipped cameras and even Information Collected through unknown sources is difficult to handle.

B. Passive Methods

Passive methods do not require any previous information about the image, and they take advantage of specific detectable changes that forgeries can bring into the image. These Blind Approaches used image statistics or content of the image to verify its genuineness.Copy Move Forgery is also an example of Passive Method.

IV. COPY MOVE FORGERY DETECTION IN DIGITAL IMAGES

An image forgery is called as Copy-Move forgery when some content (region) of an image is copied and pasted within that same image. This is usually done in order to hide some information of the image. There must be a possibility that one or more region is copied and moved into the image. As the copied part came from the same image, its important properties such as noise, color and texture do not change and make the detection process difficult. Even the detection methods must be compatible with the statistical measures presents in each part of the images that makes the detection difficult .Various Methods used in Detection are explained below:

A. Detection Based on Block Matching

Here the image is divided into blocks of equal size to bring out the features of each block. Then these features are compared with each other to find out suitable match. After finding these matches, the equal block pairs are treated as copy move.

The approach is as follows:

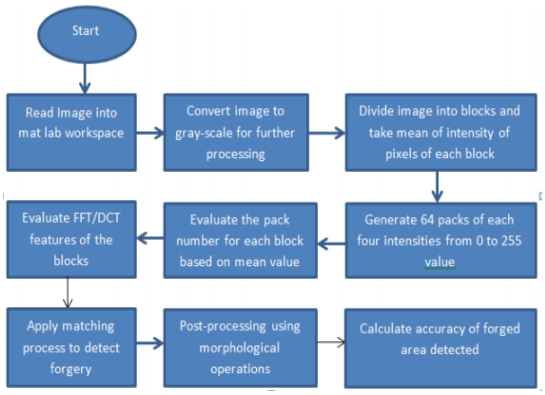

Fig.4: Flowchart for Block Based Method

B. Key Point Based Method

The existing region duplication detection methods are based on blocking matching technique, if any kind of transformation is applied into the moved region then the block matching techniques are unable to identify those type of forgeries. In this work we describe a new technique for region duplication detection. This starts by key-point based features like SIFT.To identify the key points, variouskeypoint detector algorithms are used. Then the feature extraction is performed by matching the feature vectors which is extracted from a region around these key points.In other words here the features are extracted without dividing the image the image. Here the approaches like clustering, Euclidean distance, the nearest neighbor etc. can be used for feature point matching .A forgery can befound if matching features are found. Further the variouspost processing techniques, such as RANSAC can also be used for removing false matches.

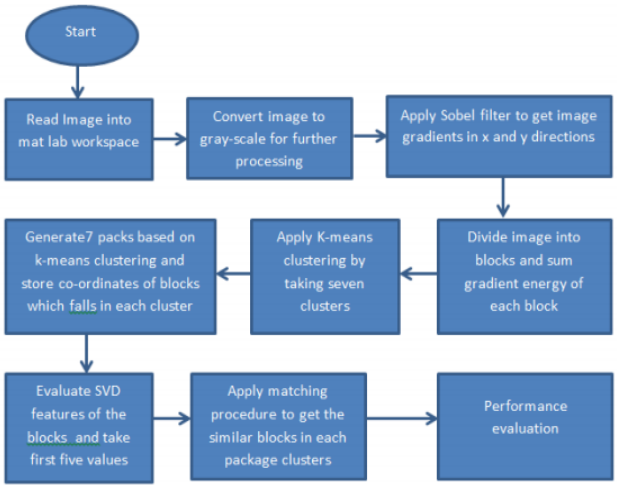

Fig.5: Flowchart for Key point Based Method

C. Edge enhancement using Gabor filtering

Small or Smooth Cloned regions are difficult to detect in copy move forgery. Due to this ,Gabor Filter is used. Gabor filters are band pass filters which are

used in image processing for feature extraction, texture analysis, and stereo disparity estimation. The impulse response of these filters is created by multiplying a Gaussian envelope function with a complex oscillation. These elementary functions minimize the space (time)-uncertainty product. By extending these functions to two dimensions it is possible to create filters which are selective for orientation. Under certain conditions the phase of the response of Gabor filters is approximately linear.

D. Working Of Gabor Filter

First the tampered image is segmented into overlapping fixed sized blocks and Gabor Filter is applied to each The image of gabor magnitude represents each block. Statistical Features are extracted from HOGM(histogram of Oriented gabor magnitude)of overlapping blocks and reduced pairs after suitable post processing. Finally Feature vectors are sorted lexicographically and duplicated image blocks are indentified by finding similar blocks .

Sobel Edge Detection Filters . A way to avoid having the gradient calculated about an interpolated point between pixels is to use 3 x 3 neighborhoods for the gradient calculations in Devadoss, C.P. Et al, 2018. Consider the arrangement of pixels are about the pixel [i, j] TheSobel operator is the magnitude (M) of the gradient computed by:

$$M_{\sqrt{}}\sqrt{s_x^2+s_y^2} \qquad (1)$$

The fractional (partial) derivatives are calculated by:

$$s_x=(a_2+ca_3+a_4)-(a_0+ca_1+a_6) \quad (2)$$

$$s_y=(a_0+ca_1+a_2)-(a_5+ca_5+a_4) \qquad (3)$$

Here the constant c=2

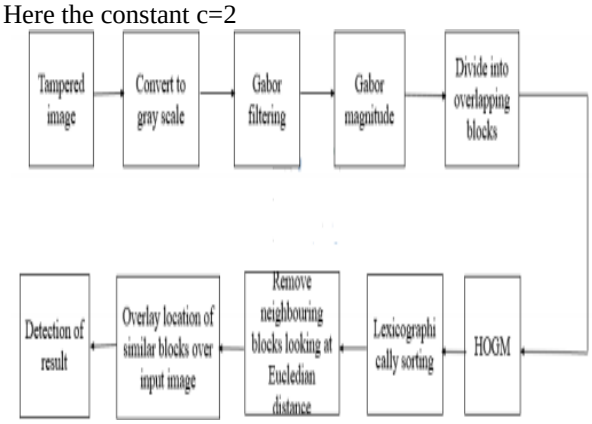

Fig.6: Block Diagram of Gabor Filter

V.PROPOSED SYSTEM MODULE

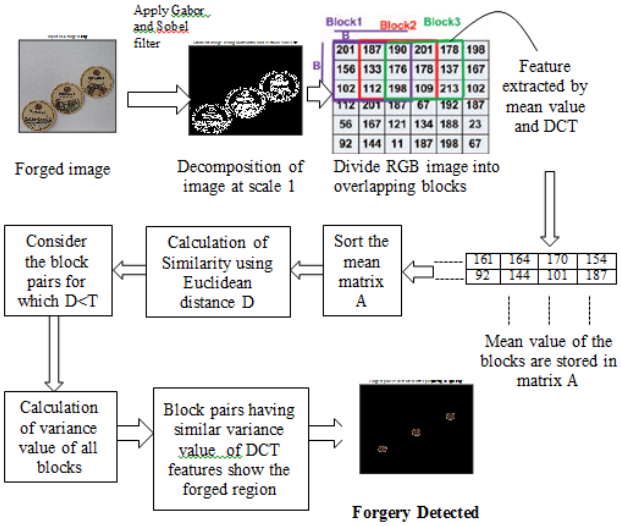

Fig.7:Proposed Module

VI.ALGORITHM USED

1.Pre-Processing

Step 1: Creating 64(256/4) packages, denoted as PA1,PA2,...,PA64, where the offset value is 4;
Step 2: Converting A 'to a gray scale image A ;

2. Feature extracting

Step 3: Getting the high and width of image A , denoted as M and N , respectively;
Step 4: Dividing A into (M-b +1) X (N-b +1) overlapping blocks, denoted as Bij, where 0< b<<M,0< b<<i< j < (N-b +1);
Step 5: For each Bij
Step 6: Applying FFT to generate its coefficient matrix, denoted as Cj ;
Step 7: Extracting its features C1, Cj, Cj, Cjj from C j ;
Step 8: Calculating the pixel mean of Bij, denoted as Pij ;
Step 9: Putting its features and coordinates into a corresponding package PAk according to Pij
Step10: End For

3. Similar region matching

Step11: For each PA
Step12: The similar block pairs will be matched according to their features and a map will be labeled with '0' or '255' according to their coordinates;
Step13: End For
Step14:Outputting the map that includes the detecting results.

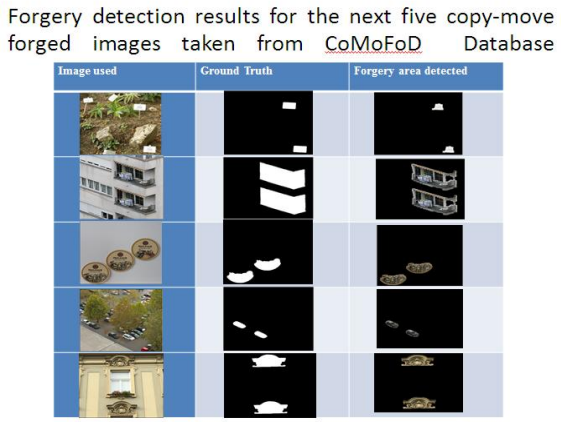

Fig 8: Detection Results

VII.PERFORMANCE EVALUATION

For performance evaluation of the proposed method, sensitivity, specificity and accuracy has been calculated for each image. First of all, Forgery detection has been extracted from whole dataset and feature extraction has been carried out using DCT and FFT texture algorithms. After that forged pixels has been calculated using both methods. The classification accuracy is the extent to which the classifier is able to correctly classify the examplars and is summarized in the form of confusion matrix to the test data. This is defined as theratio of the number of correctly classified patterns (TP and TN) to the total number of patterns (species) classified.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Sensitivity:

The sensitivity of a classifier is the fraction of the image samples correctly classified as that specific species class. It is defined by equation below :

$$Se = \frac{TP}{TP + FN}$$

Specificity:

The specificity is the fraction of normal pixels correctly classified as normal class. It is also called selectivity.

$$Sp = \frac{TN}{TN + FP}$$

VIII.ROTATION INVARIANT FEATURE EXTRACTION METHODS

Till the methods described above, only basedon copy move detection but when various geometric transformations are appliedon these images like rotation ,scaling bluring,it createsproblem.To overcome these,we explore some methods which are rotationinvariant..Both methods (PZM-based and ZM-based) are strong against blurring, noise adding, color reduction, brightness change, and contrast, adjustments.HereRotation using Pseudo-Zernike Moment (PZM) and Zernike Moments (ZM) in detecting copy move forgery are tested. For evaluating the performance of these methods, inclusive and reliable dataset COMOFOD database [26], which consists of 260 forged imagesis used for testing purposes. PZM-based method is somewhat faster and more perfect than Z based method.

A. PZM-based Copy-Move Detection Method

Firstly,the RGB color image is converted into gray-scale image and resized (scale down) to be 512*512 as a preprocessing step. This is because gray-scale image is easy to boost and interprets. Further the image with size N×N is divided into overlapping blocks of size B×B, assuming that the pre-defined size of a block is smaller than the tampered region. The number of blocks (N of B) equal (N– B+1)×(N–B+1). Vector is calculated for each and every block and is stored in a 2-D array(PZ) . PZ is lexicographically sorted in, so that blocks with same features become close to each other. For every two neighboring blocks in the sorted array compute the Euclidian distance and the Physical distance (PhDist) between them. The adjacent block in the sorted array could be the next between them. EDist and PhDist can be calculated. If the tested pair fulfils the following two conditions, then they are nominee to be a copy move case (i.e., duplicated parts). EDist is smaller than a pre-defined threshold D1 (EDistD2). Here, D2 is related to block size (B). All candidates blocks caused from the previous step update the shift vector. The shift vector maintain a counter for each (row, column) shift. This counter represents number of replicatedregions that have the same shift. Finally, all candidate blocks (step 6) having their shift gain a counter greater than a predefined threshold (C) are described as a copied region. This can be ended by coloring them with a similar color.

B. Testing Pseudo-Zernike Moment-based Method

Under this , 50 forged images without any changes(i.e., no modification is applied on the copied region) were selected. Here we take an example of forged image where a tree branch from the original image is glued in the same image to fleece some cars,that's why some parts of tree branch are colored in orange. These orange parts indicate that these are duplicated. PZM-based method is able to find -with a high accuracy- the forged regions even if they were: Too small,toolarge,duplicated many times or one different region copied and pasted in same image again and again as shown in **fig.9(b,c,d,e).**

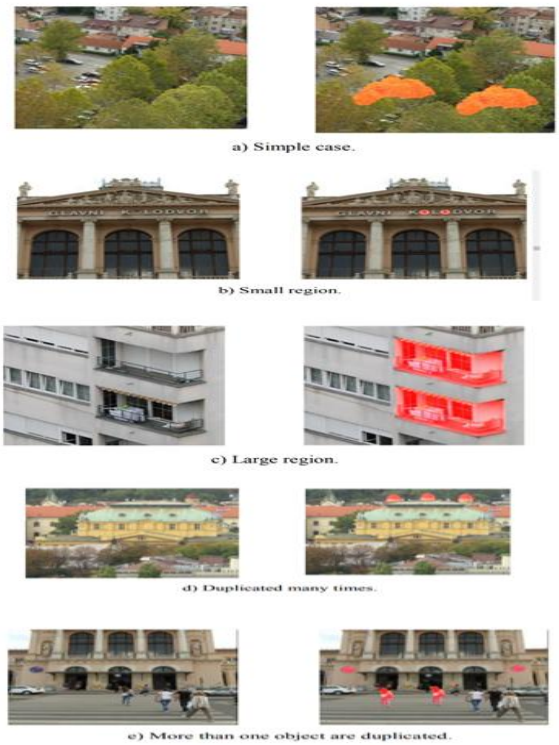

Fig.9(b,c,d,e):Detection of Forgery Using PZM Based Method

IX.POST PROCESSING METHODS

Here,five different types of post processing methods were applied on images in COMOFOD database. These methods are robust against noise adding, image blurring, brightness change, color reduction and contrast adjustmentsas shown in **Fig 10**

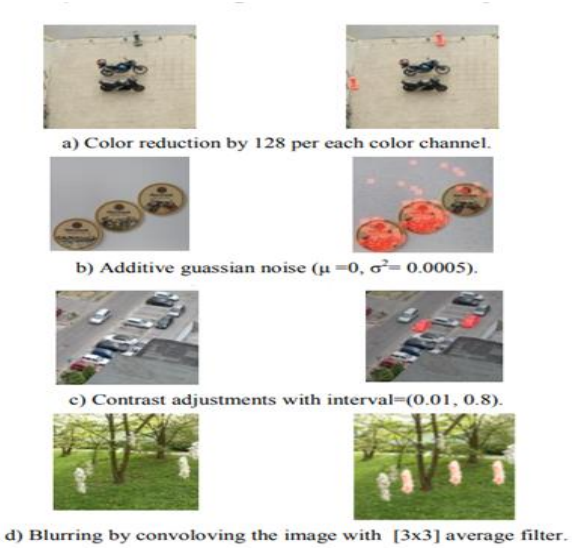

Fig.10:Post Processing Methods

Rotation and Scaling: In this portion, the algorithm is tested against rotation means-a copied region is rotated and translated to a new location; and inscaling-a copied region is scaled and translated to a new location. Under this, copied region is affected by rotation with different angles. Results were not perfect but they are acceptable as shown in **Figure11**. Scaling: In this we show how copied region is affected by scaling with different scaling ratio.

Rotation and Scaling

Fig.11: Rotation and Scaling

X.COMPARISONS BETWEEN PSEUDOZERNIKE MOMENTS AND ZM-BASED METHODS

ZM-based method and PZM based method are very good in detecting copy-move forgery for those images that are not affected by any modification, but for images that are affected by rotation, scaling, blurring … etc., PZM gives better results in less time. In most cases PZM-based method need few time to identify the fake parts as compared to ZM-based method. PZM-based method can find the forged parts using moment of order (n=1) in 126 second, while ZM-based method can find the forged parts using moment order (n=2) in 144 second. Even for the images that areaffected by rotation and blurring, PZMbased method gives more correct results than ZM-based method.

XI. CONCLUSION

Till this time, we have implemented three block based CMFD techniques which uses DCT,FFT and SVD features when forgery is detected based on matching process. First method generates 64 clusters in which individual blocks has been noted based on mean values of the intensity pixels in the blocks. The algorithm takes much time in computation because of matching of large no. of blocks to one another. Second method generates only seven clusters based on k-means clustering which uses gradient energy of the blocks as input. Some blocks have been discarded in matching process as there are no edges in those regions. Hence decreases the computation time. Further,another method is described in which sobel and gabor filter based edge detection is carried and matching process is carried out for those pixel blocks only which are edge pixels. This results in least computation time in forgery detectionAs these

algorithms are efficient only for copy-move, they need to be amended to work on rotated of copy move regions in the image. Hence future work will be to explore those feature extraction methods which are rotation invariant. Experimental results has been carried out on CoMoFoD Database [] which contains different types of forged images. Further Rotation Invariant Forgery Detection Method using Zernike Moments has been proposed. The results showed that PZM-based method can detect all forged images without any pre/post processing with accurate results, all forged images with more than one copied object. It is robust against contrast adjustments and color reduction.

REFERENCES

[1] Math, S. &Tripathi, R. C. (2011). Image quality feature based detection algorithm for forgery in images. International Journal of Computer Graphics and Animation (IJCGA), 1, 13-21

[2] Singh, V. K. &Tripathi, R. C. (2011). Fast and Efficient Region Duplication Detection in Digital Images Using Sub-Blocking Method. International Journal of Advanced Science & Technology, 35, 93-102.

[3] Z. Junliu ; G Yanfen (2016),. Detection of copy–move forgery using discrete analytical Fourier–Mellintransform.Nonlinear Dynamics April 2016, Volume 84, Issue 1, pp 189–202

[4] Ryu, S. J., Lee, M. J. & Lee, H. K. (2010). Detection of CopyRotate-Move Forgery Using Zemike Moments. Springer, Information Hiding Lecture Notes in Computer Science, 6387, 51- 65.

[5] XiuliBi, Chi-Man Pun, Xiao-Chen Yuan (2016). Multi-Level Dense Descriptor and Hierarchical Feature Matching for Copy–Move Forgery Detection. published in Information Sciences 345(2016) 226–242

[6] Dr. S.D. Chede, Prof. P.R.Lakhe(2015). Forgery of Copy Move Image Detection Technique by Integrating Block and Feature Based Method. International Journal of Advanced Research in Computer and Commu(2013). Copy-Move Forgery Detection using DCT and SIFT. International Journal of Computer Applications (0975 – 8887) Volume 70– No.7, May 2013

[7] Huan Wang, Hong-Xia Wang, Xing-Ming Sun, Qing Qian (2017). Passive authentication scheme for copy-move forgery based on package clustering algorithm. published in Multimedia Tools and Applications May 2017, Volume 76, Issue 10, pp 12627–12644

[8] Khana, A., Malika, S. A., Alib, A., Chamlawia, R., Hussaina, M., Mahmoodc, M. T. &Usmand, I. (2012). Intelligent Reversible Watermarking and Authentication: Hiding Depth Map Information for 3D Cameras. Elsevier, Information Science, 216, 155—175.

[9] Hsiao, J. H., Chen, C. S., Chien, L. F. & Chen, M. S. (2007). A New Approach to Image Copy Detection Based on Extended Feature Sets. IEEE Transactions on Image Processing, 16, 2069-2079.

[10] Ling, H., Cheng, H., Ma, Q., Zou, F. & Yan, W. (2012). Efficient Image Copy Detection Using Multiscale Fingerprints.IEEE Multimedia, 19, 60- 69.

[11] Nikolopoulos, S., Zafeiriou, S., Nikolaidis, N. & Pitas, I. (2010). Image Replica Detection System Utilizing R-trees and Linear Discriminant Analysis. Elsevier Pattern Recognition, 43, 636-649.

[12] D. Tralic, I. Zupancic, S. Grgic, and M. Grgic, ―CoMoFoD-New database for copy–move forgery detection,‖ in 55th IEEE International Symposium ELMAR 2013.

[13] DijanaTralic; Sonja Grgic; XianfangSunPaul ; L. Rosin (2016). Combining cellular automata and local binary patterns for copy-move forgery detection.Multimedia Tools and Applications Dec,, Volume 75, Issue 24, pp 16881–16903

[14] Hu, WC., Chen, WH., Huang, DY. et al. (2016). Effective image forgery detection of tampered foreground or background image based on image watermarking and alpha mattes.Multimed Tools Appl (2016) 75: 3495.

[15] Lien, C. C., Shih, C. L., & Chou, C. H. (2010). Fast forgery detection with the intrinsic resampling properties. International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 232-235

[16] Hajihashemi V., Gharahbagh A.A. (2018) A Fast, Block Based, Copy-Move Forgery Detection Approach Using Image Gradient and Modified K-Means. In: Thampi S., Mitra S., Mukhopadhyay J., Li KC., James A., Berretti S. (eds) Intelligent Systems Technologies and Applications. ISTA 2017.Advances in Intelligent Systems and Computing, vol 683. Springer, Cham

[17] Devadoss, C.P. &Sankaragomathi, (2018) "Near lossless medical image compression using block BWT–MTF and hybrid fractal compression techniques" Cluster Computing pp 1–9.