IJCAT - International Journal of Computing and Technology, Volume 5, Issue 11, November 2018
ISSN (Online) : 2348-6090
www.IJCAT.org
Impact Factor: 0.835

DFE Approach for CMFD on Digital Images – A Review and Performance Evaluation

[1]Arun Anoop M, [2]Poonkuntran S

[1] Ph.D. Scholar, COMPUTER SCIENCE AND ENGINEERING, VELAMMAL COLLEGE OF ENGINEERING AND TECHNOLOGY, VIRAGANOOR, RAMESWARAM HIGHWAY,MADURAI, TAMILNADU, INDIA

[2] PROFESSOR AND HEAD, COMPUTER SCIENCE AND ENGINEERING, VELAMMAL COLLEGE OF ENGINEERING AND TECHNOLOGY, VIRAGANOOR, MADURAI, TAMILNADU, INDIA

Abstract - In today's advanced age the reliable towards picture is twisting a direct result of malicious forgery images. The issues identified with the security have prompted the examination center towards tampering detection. As the source image also, the objective locales are from a similar picture so that copy move forgery is very effective in image manipulation due to its same properties such as temperature, color, noise and illumination conditions. In this article, we added preliminary research methods (existing algorithms). We used hybrid approaches of existing algorithms. The performance is evaluated in terms of normally used parameters precision and recall with improved results. Thus, the proposed CMFD can manage all the image processing operations. Finally made a comparative analysis based on some parameters.

Keywords: *Copy move forgery detection(CMFD), Zernike Moments(ZM), Weber Local Descriptors(WLD), copy move forgery, block-based, feature extraction, matching, tampering.*

1. Introduction

Digital images forgeries happening because of lack of security between client and server. In medical field, medical image manipulation occurred, is that the security less communication channel between hospital and patient(s). If any manipulation of data may life threaten patient's health. But nowadays many illegal manipulations in images and videos we can see. Digital image are used in some of the medical, court. Copy move forgery (CMF) is one of the particular form of image tampering where a piece (interested potion) of the image is copy-pasted on other piece of the same image. Digital image forgery, were because free available image editing tools like Adobe photo shop , GIMP etc. [1] . Cut a piece of leaves and pasted it to hide any of the object is Copy Move Forgery. Musaed Alhussein mentioned to include feature selection algorithms to reduce the number of features. Also, in the future, authors will investigate the effect of other types of color components such as luminance and Chroma, or hue and saturation, in image forgery detection [2]. Vincent Christlein et. al., develop a joint forensic toolbox performs on manipulated images [3]. V.Suresh et. al., mentioned in future authors will concentrate to detect spliced images [4]. Meenal Shandilya mentioned in future author will add identification of other forms of geometric attacks, relevant to copy-move forgery, such as reflection, as well as other image region transforms, such as gray level interpolation [5]. Anushree U. Tembe et. al., mentioned to find tampered regions with other type of geometric transformations in future [6]. Rani Susan Oommen et. al., use a different measure instead of SSIM to localize forged regions to get efficient detection. Authors mentioned SSIM is not a good measure to compare regions [7]. R.C. Pandey et. al., mentioned in future their work will detect splicing in human body and face, to concentrate social networking sites using different image features [8].

2. Related works

Anil Dada Warbhe et. al., concluded the main drawback of block-based approaches. Authors mentioned that the detection procedure of copy-move forgery took high computation time. Authors concluded that in block-based approach, the image needs to be divided into the number of blocks and each block is processed for feature extraction and matching. Hence authors best choice is key-point based approach for copy-paste forgery detection in large size images over block based approach [9]. Yongzhen Ke et. al., mentioned Image recognition accuracy, common sense knowledge and refinement of logic reasoning rule was not high enough. And they concluded that improving accuracy will be their future works [10]. Xunyu Pan et. al., robustness of the proposed algorithm with regards to several imaging conditions. And authors future work will

Combine the current detection method with other noise based features to increase the detection performance [11]. P M Panchal et. al., mentioned future work will be in video registration [12]. SITI FADZLUN MD SALLEH et. al., mentioned future works may explore in color images, or high resolution images. And also future works should consider multilayer processing [13]. Geethu N Nadh et. al., mentioned authors will think about to add security enhancements in future [14]. Nishmitha M.R et. al., mentioned to add DWT to detect image forgery in future [15]. SeungJin Ryu et. al., mentioned to concentrates on establishing an appropriate data structure [16]. Keerthi Priya et. al., mentioned their work can be implemented in real applications. Also, authors have an idea to combine with other mechanisms like image segmentation and neural learning [17]. Hansoo Kim et. al., mentioned to include implementations and verifications of several detection schemes of digital image forgeries [18].

3. Problem Definition

Main problem is lack of security between client and server. Most important problem is authenticity. Main drawback is a person who have well knowledge in manipulation, he or she can change normal image to abnormal and abnormal to normal. This will increase the crime rates. A small bit change can identify by image forgery detection approach.

4. Proposed System

The research work of the paper is to identify the tampered portion of the image. The proposed work consists of three main steps(ii-iv):
(i) pre-processing, (ii) Block Tiling, (iii) Feature Extraction, (iv) Block Matching and (v) Block reconstruction.

In proposed system (Multiple Feature-Extraction Approach) is implemented based on 2 existing algorithms. And we used fusion approaches for evaluation process (both keypoint and block-based) before our experimental work.

4.1. Input Data Base

The information images gathered from various website pages is considered as database for the proposed system.

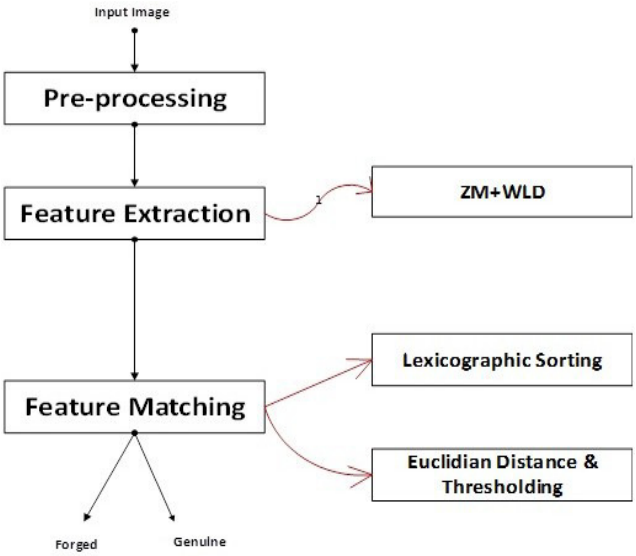

Fig. 1 Proposed Block Diagram

4.2. Preprocessing: Below mentioned are usual steps we can see in every papers. There is no noval methods mentioned in this section.

- Read the original image from the database.
- After that the original RGB image is converted into Gray scale image using standard color space conversion.
- In color image processing, no need any type of conversion. Gray conversion can identify more accurate features from corners.
- Below mentioned is the Standard equation .The standard equation is to convert RGB to Grayscale.
- In the below equation (1), R, G and B are red, green and blue components.
- The standard equation from RGB to Gray conversion is,

$$I_g = 0.229R + 0.587G + 0.114B \quad (1)$$

4.3. Block Tiling

After pre-processing, the picture is separated into small squares.

4.4. Feature Extraction: Below mentioned are usual steps we can see in every papers. There is no noval methods mentioned in first and second bullet notation section. Our contribution is we just taken ZM and WLD algorithms to extract features for CMFD.

- The extraction of relevant information that represent the characteristics features of the image.
- Feature vector's size will depend on the block size.

- After that the features of the blocks are extracted using Zernike Moment, Weber Local descriptor.

4.4.1 Zernike moments[21] :

- are exact descriptors even with relatively few values which is defined on a unit circle[21] with set of orthogonal polynomials[21],[22-23]
- There are two basic steps which can be used to convert the rectangular region of each image to a unit circle[21].

4.4.2. Weber Local descriptor [25]:

- A dense descriptor inspired by weber`s law, a robust and most powerful local descriptor called Weber Local Descriptor is introduced.
- It employs both the advantages of LBP (Local Binary Pattern) and SIFT(Scale Invariant Feature Transform).
- LBP must be computationally efficient and having smaller support regions [25].

4.5. Block matching: Below mentioned are usual steps we can see in every papers. There is no noval methods mentioned in this section(next two bullet notation).

- After feature extraction, normally everyone uses the block matching stage. That stage will find out the similarities between features in the image.
- In that step, the features are arranged on a lexicographical order.
- Technique that used for sorting called lexicographical sorting.

Usual procedure to find out the feature vector of all the blocks within a matrix (Fig 4.) form.

Finally, find the similar blocks with minimum Euclidean distance. 'Euclidean distance' to identify the manipulated part in an image.

- The distances between two equivalent image squares in the Euclidean space.
- The distance between the similar overlapping blocks to identify the forgery.

Here we used feature matching procedure to find out the matching between features. Here we describe the feature matching procedure based on HOG algorithm.

- In our work, `feature extraction` procedure, the following are the steps(Example of HOG Feature Extraction and matching).

For original image,

[HOG feat1]=hog feature vector(RGB1);\

For forged image,

[HOG feat2]=hog feature vector(RGB2);

Where, hog feature vector has to download from math-works site and keep it in the same folder. In our work, `feature matching` procedure, the following are the steps.

```
HOG m=0
[row,column]=size(HOG feat1);
For i=1 to row h
For j=1 to column h
    if(HOG_feat1(i,j)===HOG_feat2(i,j))
      HOG m=HOG m+1;
    end
   end
end
```

4.6. Block Reconstruction

The reconstructed images f^∧ (u,v) can be generated from four features as,

$$f^{\wedge}(u,v) = \sum_{x=0}^{x_{max}} \sum_{y=0} ZM_{xy}, WLD(\xi,\theta))$$

(2)In ZM, the Highest degree of moments is 12[6].

5. Results

- The proposed work is implemented in the MATLAB 2014a software with a database of images. In this work, the image is taken from the Columbia university dataset [20].

5.1 Result Analysis

5.1.1 Performance Evaluation

- The step by step analysis part of the proposed forgery detection is mentioned below with three original images shown in Figure 5.
- The original image is the RGB image so that Gray scale conversion is carried out will be shown in Figure 6.
- A particular part of the image is taken from the image and pasted into the same image for tampering the image. After selecting the particular

region that region is rotated to a certain angle and pasted in the image as forgery will be represented in Figure 7. Then the image will be as the forgery image or tampered image.

- The forgery detected part of the image is mentioned in figure 8-9. The performance is evaluated in terms of precision and recall to show the robustness and accuracy for the forgery detection.
- In our next work, we will evaluate the same to test for robustness, effectiveness, accuracy against attacks like AWGN, Gaussian Blur, Gaussian Noise, rotation (Image transformations).In our next work these image transformations will notate as "clue removal attacks".

5.2 Evaluation Metrics

The performance evaluation of the proposed work is evaluated in terms of the following:-

5.2.1 Precision(Defintion- Below mentioned are usual steps we can see in every papers. There is no new methods mentioned in this definition and standard equation of "precision" section. These are all the predefined performance measures):

- "Precision can be measured as the ratio of number of images that can be detected correctly as forged to the sum of number of images identified as forged and the wrongly identified as forged".
- Precision=((T_p)/(T_p+F_p)) × 100 (3)

Where T_p is the true positive rate and F_p is the false positive rate.

5.2.3. Recall (Definition- Below mentioned are usual steps we can see in every research papers. There is no noval methods mentioned in this definition and standard equation of "recall" section. These are all the predefined performance measures): "The ratio of detected parts correctly to the sum of the tampered parts not been correctly detected and the parts detected correctly using the algorithm".

- Recall=((T_p)/(T_P+F_N))×100 (4)

The performance of the proposed forgery detected image is verified in terms of precision, recall measures. The performance is evaluated for three images.

Thus, the copy move forgery detection of the proposed work will provide better performance as compared to the HOG in terms of precision and recall.

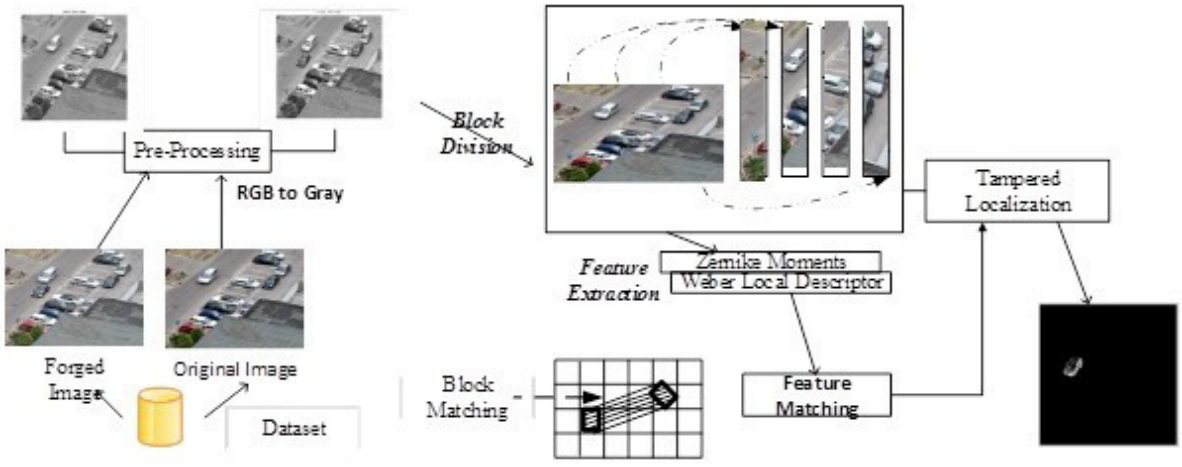

Fig. 2 DFE Approach (Block diagram of the proposed work): Dual Approach (Block diagram of the proposed work{ZM+WLD})

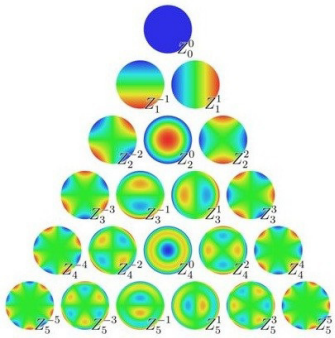

Fig. 3 Zernike Moments [24]

$$FM = \begin{bmatrix} f_{11} & f_{12} & f_{13} & f_{14} \\ f_{21} & f_{22} & f_{23} & f_{24} \\ \vdots & \vdots & \vdots & \vdots \\ f_{(U-u+1)\times(V-v+1)} & f_{(U-u+1)\times(V-v+1)} & f_{(U-u+1)\times(V-v+1)} & f_{(U-u+1)\times(V-v+1)} \end{bmatrix}$$

Fig. 4 The feature vector of all the blocks within a matrix

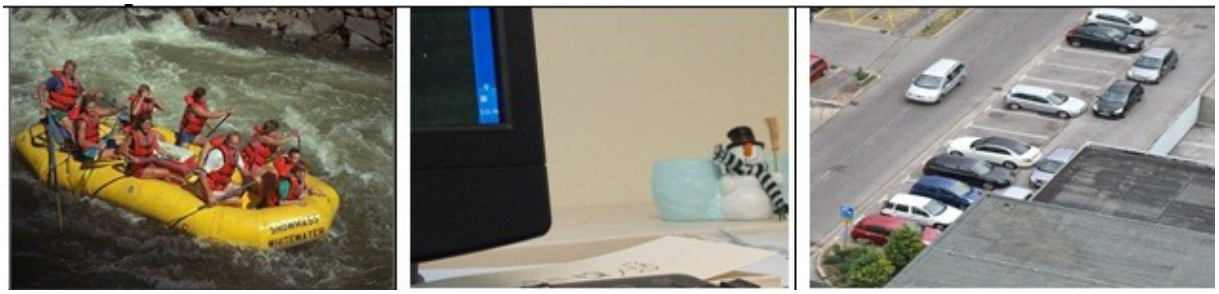

Fig. 5 Original Images (a) Kodak Dataset Image (b)Columbia University Db (c)CoMoFoD dataset

Fig. 6 Grayscale conversion of original Images (a) Kodak Dataset Image (b)Columbia University Db (c)CoMoFoD dataset

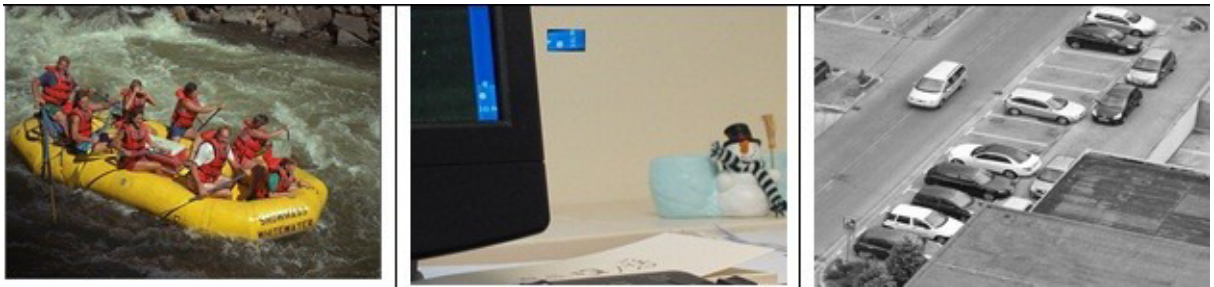

Fig. 7 Forged Images (angle=Left 90)

Fig. 8 Authenticity of Images (Forgery detected area)

Fig. 9 Multiple Forged pictures

Fig. 10 Authenticity of Images (Multiple Forgery detected area)

Table 1: Performance metrics comparison for forgery detection

Images	***Precision***	***Recall***
Image1	50	100
sImage 2	50	98.2
Image 3	100	96.8

Table 2: Performance metrics comparison for forgery detection using methods

Techniques	***Precision***	***Recall***
HOG[51]	90	82

HOG[29]	93	87.2
Proposed(ZMWLD)	100	97.4

5.3 Comparative analysis

Fig. 13 Copy Move Forgery Example[48,50]

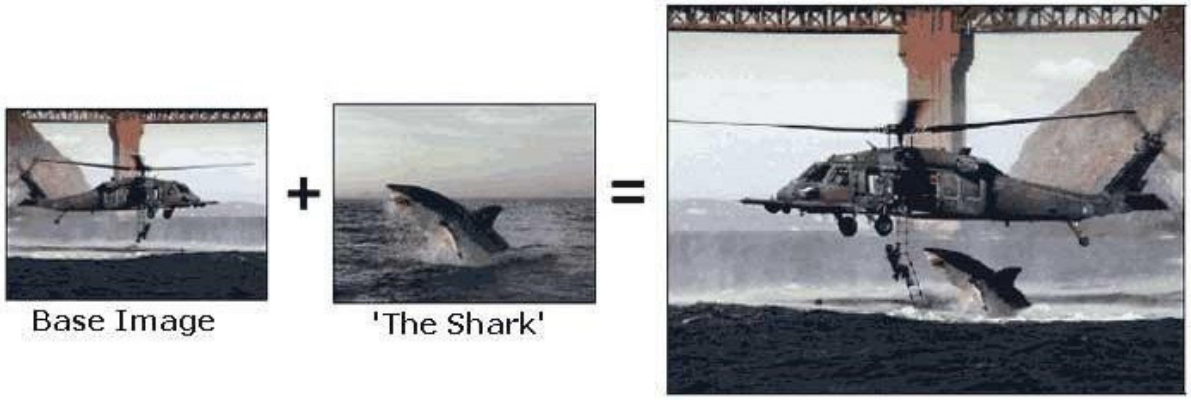

Fig. 14 Image Splicing Example[48-49]

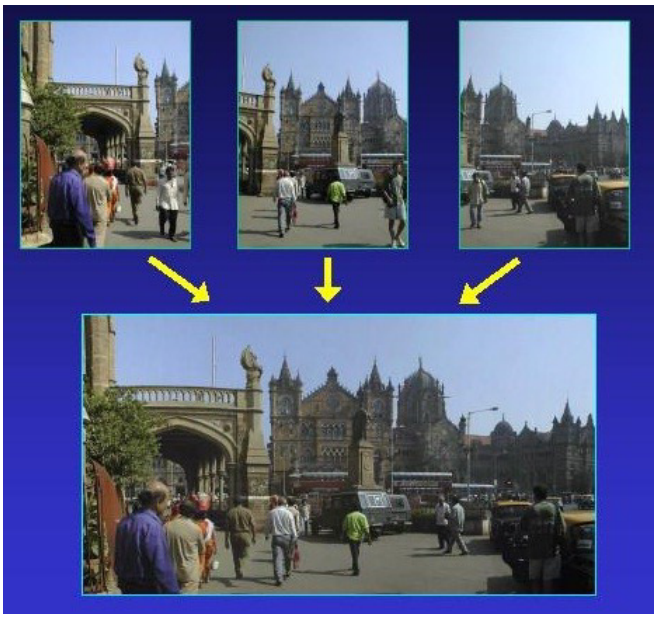

Fig. 15 Image Compositing Example

$$r_{1,2} = \frac{C(I_1, I_2)}{mean(m_1, m_2)}$$

(5) [27]

$$CDR = \frac{|C \cap \tilde{C}| + |F \cap \tilde{F}|}{|C| + |F|}$$

$$FDR = \frac{|\tilde{C} - C| + |\tilde{F} - F|}{|\tilde{C}| + |\tilde{F}|}$$

(6) [26]

Table 3: Analysis study of Image Forgery types

Sl.No:	***Image Forgery Types***	***Description***	***Original and Forged Image***
1	Copy Move	Copying regions of the original image and pasting into other areas. The yellow area has been copied and moved to conceal the truck [23].	Figure 13
2	Splicing	Joining 2 or more images and produce on [28].	Figure 14
3	Image Compositing	This is a technique used to composite multiple images into a single image. The image compositing is also known as photomontage and image splicing [29] .	Figure 15

Table 4: Analysis study of CMFD Techniques

Sl.No:	***CMFD Types***	***Algorithm***

1	"Pixel based FD"	Consists of Cloning, Splicing, Resampling [35].
2	"Camera based FD"	Consists of Chromatic, Sensor Noise, Camera Response [35].
3	"Format based FD"	Consists of Double JPEG, JPEG blocking, JPEG Quantification [35]

Table 5: Analysis study of "post processing steps"

Sl. No:	*CMFD Types*	*Algorithm*
1	[30]	Authors calculated Correct and False detection ratio. They mentioned analyzed sub block sizes 16X16, 32X32, 48X48 Pixels. They done analysis of robustness against Translation, Scaling, Blurring, Altered brightness, Color reduction. And they used CoMoFoD database[30].
2	[31]	Author(s) used USC-SIPI database. Calculated Precision and Recall and calculated DAR, FPR. They analyzed based on Effectiveness, Accuracy test and Robustness test. In that tampered images distorted by Gaussian Blurring, AWGN,JPEG Compression [31].
3	[32]	Author(s) randomly taken 50 images from USC-SIPI database and Kodak website of 32X32 Pixels. And they calculated DAR and FPR for Accuracy test and Robustness test. Tampered images distorted by Gaussian Blurring, AWGN, JPEG Compression for pixels of 32X32,64X64[32].
4	[33]	Authors taken 200X200 pixels images from Google Image search and forged with the help of Adobe Photoshop. They calculated Accurate detection, False detection. Effectiveness test for authenticity assurance[33].
5	[34]	Author(s) used USC-SIPI database and Kodak database. And calculated Precision and Recall. And also calculated DAR, FPR for Effectiveness, Accuracy test and Robustness test. Tampered images distorted by Gaussian Blurring, Additive White Gaussian Noise (AWGN),JPEG Compression[34].

Table 5: Available Dataset Details

Dataset Name
Columbia University Datatset[38]
CASIA Dataset [39]
CoMoFoD dataset [37]
Kodak dataset [36]
USC-SIPI dataset [40]

Table 6: Analysis study of Different Measures

Sl.No:	*Author name*	*Metrics Information*
1	Luo Juan	Luo Juan et. al., mentioned some metrics. "That are,
		Repeatability measurement,
		[equation 5]
		And difference-of-Gaussian function(DoG), Time , Scale,
		Rotation, Blur, Illumination and affine[27]".
2	Chen-Ming Hsu	[equation 6]
		"Correct detection ratio (CDR)and False detection ratio
		(FDR), Where C is the copy region, F is the tampered region,
		and C' and F' are the detected copy region and the detected tampered region, respectively. — —refers to the area of the region, ∩refers to the intersection of two regions, and – refers to the difference between two regions"[26].

Table 7: Analysis study of some Feature Extraction methods

Sl. No:	*Feature Extraction methods*	*Algorithm*

1	HOG[40]	HOG feature descriptor used for person on foot location detection[40].
		HOG is Histogram of Gradients[40].
		○ Gradient Computation[41-42]: ✓ Find both the level and vertical bearings(Ix and Iy)[41-42], $D_X = [-1 \quad 0 \quad 1]$ $D_Y = [-1 \quad 0 \quad 1]^T$ (3)
		○ Orientation Binning and Descriptor Block[41-42]: ✓ Next is to find the angle and magnitude value. ✓ Bin in the range 0 to 180 degrees[42]. ✓ From these will get the block features[41].
2	GLCM[43]	It is a classification of how regularly unique combinations of pixel splendor esteems (dark levels) occur in an image[43].
		GLCM is Gray-level co-occurrence matrix[43].
		$GLCM_{i,j} = \{C_{i,j}, E_{i,j}, CO_{i,j}, H_{i,j}\}$ (4) And some calculations are below, $E = \sqrt{\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} M^2(i,j)}$ (5) $C = \sqrt{\sum_{i=0}^{N-1}(\sum_{j=0}^{N-1}[\{(ij)M(i,j) - u\_x, u\_y\}/\{s\_x, s\_y\}])}$ (6) $H = \sqrt{\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} M(i,j)/(1+(i-j)^2}$ (7)
3	Jeffry's Image metadata viewer[45].	Can't identify MS Paint used forgeries. Online tool for viewing metadata embedded within images, such as camera setting used when taking a photographs, date and location[45].
4	Hex editor[47].	A hex editor is a type of computer program that allows for manipulation of the fundamental binary data that constitutes a computer file[47].
5	EXIFTool by Phil Harvey[46].	ExifTool is a free and open-source software program for reading, writing, and manipulating image, audio, video, and PDF metadata [44]. Other methods to remove EXIf are [46].

6. Conclusions

Thus, the paper solved the problem of image authenticity using the combination of Zernike Moments and Weber local descriptors. DFE approach will work only if we have 2images (original and forged). Two feature extraction combination is our preliminary approach. In the future, we will apply clue removal attacks also before post processing stage. In our next work, we will deal with the same to test for robustness, accuracy tests against attacks like AWGN, Gaussian Blur, Gaussian Noise, rotation (Clues removal attack once normal image processing attacks finished). And we will deal with medical images like mammograms and radiographic images like x-ray images and assure authenticity of images.

References

[1] Arun Anoop M, "Image forgery and its detection: A survey", 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS),IEEE, March 2015.

[2] Vincent Christlein, Christian Riess, ,Johannes Jordan, Corinna Riess, and Elli Angelopoulou," An Evaluation of Popular Copy-Move Forgery Detection Approaches",IEEE

TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY,26 Nov 2012.

[3] V.Suresh, T.Primya, G. Kanagaraj," Efficient Detection Technique for Image Forgery", International Journal of Imaging Science and Pattern Recognition Volume 1 Issue 1,2017.

[4] Meenal Shandilya, Ruchira Naskar, " Detection of Geometric Transformations in Copy-Move Forgery of Digital Images", Master Thesis, NIT,Rourkela,June 2015.

[5] Anushree U. Tembe, Supriya S. Thombre," Copy-Paste Forgery Detection in Digital Image Forensic", IJSRSET | Volume 3 | Issue 2,2017

[6] Rani Susan Oommen and Dr. Jayamohan M," A HYBRID COPY-MOVE FORGERY DETECTION TECHNIQUE USING REGIONAL SIMILARITY INDICES", International Journal of Computer Science & Information Technology (IJCSIT) Vol 7, No 4, August 2015

[7] R.C. Pandey, S. K. Singh, and K. K. Shukla," A FULLY AUTOMATED BLIND AND PASSIVE FORENSIC METHOD FOR IMAGE SPLICING DETECTION", I J C T A, 9(41) 2016, pp. 899-908

[8] Anil Dada Warbhe, R. V. Dharaskar, V. M. Thakare," A Survey on Keypoint Based Copy-Paste Forgery Detection Techniques", International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA(ScienceDirect, Procedia Computer Science 78 (2016) 61 – 67).

[9] Yongzhen Ke, Weidong Min, Fan Qin, Junjun Shang," Image Forgery Detection Based on Semantics", International Journal of Hybrid Information tehcnology,vol.7, No.1 (2014),pp. 109-124

[10] Xunyu Pan. Xing Zhang, Siwei Lyu, " Exposing Image Forgery with Blind Noise Estimation", MM&Sec'11, ACM, September 29–30, 2011, Buffalo, New York, USA.

[11] P M Panchal, S R Panchal, S K Shah," A Comparison of SIFT and SURF", International Journal of Innovative Research in Computer and Communication Engineering,Vol. 1, Issue 2, April 2013

[12] SITI FADZLUN MD SALLEH, MOHD FOAD ROHANI, MOHD AIZAINI MAAROF,"COPY-MOVE FORGERY DETECTION: A SURVEY ON TIME COMPLEXITY ISSUES AND SOLUTIONS", Journal of Theoretical and Applied Information Technology 15th June 2017. Vol.95. No 11.

[13] Geethu N Nadh, Sreelatha S.H," Contrast Enhancement Detection on Digital Images - A Survey", International Journal Of Engineering And Computer Science ISSN:2319-7242 , Volume 4 Issue 7 July 2015, Page No. 13465-13467.

[14] Nishmitha M.R and Aravind Naik,"COMPARISON OF THREE TECHNIQUES OF IMAGE FORGERY DETECTION", International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE),ISSN: 0976-1353 Volume 14 Issue 2 –APRIL 2015.

[15] Seung-Jin Ryu, Min-Jeong Lee, and Heung-Kyu Lee," Detection of Copy-Rotate-Move Forgery Using Zernike Moments", LNCS 6387, pp. 51–65, 2010

[16] Keerthi Priya, Vishnukanth Karwa P," A Novel Image Localization Method for Image Forgery",IJIRCCE, Vol. 5, Issue 5, May 2017

[17] Hansoo Kim and Joong Lee," An Implementation and Pragmatic Analysis of the Digital Image Forgery Detection Schemes", International Journal of Future Computer and Communication, Vol. 4, No. 5, October 2015

[18] Musaed Alhussein," Image Tampering Detection Based on Local Texture Descriptor and Extreme Learning Machine", 2016 UKSim-AMSS 18th International Conference on Computer Modelling and Simulation.

[19] Ng TT, Chang SF, Hsu J, Pepeljugoski M. "Columbia photographic images and photorealistic computer graphics dataset." ADVENT, Columbia University, Technical Report. 2005.

[20] Michael V. Boland,2Mia K. Markey,1and Robert F. Murphy1*, ``Automated Recognition of Patterns Characteristic of Subcellular Structures in Fluorescence Microscopy Images,`` 1998 Wiley-Liss, Inc., RECOGNITION OF CELLULAR LOCALIZATION PATTERNS, pp366-375.

[21] Arun Anoop M, Poonkuntran S, ``Certain investigation on Biomedical impression and Image Forgery Detection,`` International Journal of Biomedical Engineering and Technology (Inderscience.)

[22] Arun Anoop M, Poonkuntran S, ``A Brief study on "Multimedia Security" In Research``, ISBN-13:978-93-86258-63-2, FIRST EDITION,JULY 2017,VSRD Academic Publishing.

[23] Michael Vorobyov,``Shape Classification Using Zernike Moments, ``Available: https://www.slideserve.com/rivka/shape-classification-using-zernike-moments.

[24] Jie Chen,Shiguang Shan, Chu He, Guoying Zhao,Matti Pietikainen, Xilin Chen, Wen Gao,``WLD: A Robust Local Image Descriptor,``IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 32, NO. 9, SEPTEMBER 2010, pp 1705-1720.

[25] Chen-Ming Hsu, Jen-Chun Lee, Wei-Kuei Chen," An Efficient detection algorithm for Copy-Move Forgery",IEEE, 2015 10th Asia Joint Conference on Information Security, DOI: 10.1109/AsiaJCIS.2015.16

[26] Luo Juan, Oubong Gwun," A Comparison of SIFT, PCA-SIFT and SURF", International Journal of Image Processing (IJIP) Volume(3), Issue(4).

[27] Anuja Dixit , Rahul Dixit and R. K. Gupta," DCT and DWT Based Methods for Detecting Copy-Move Image Forgery: A Review", International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.9, No.10, (2016), pp.249-258.

[28] Shrishail Math and R.C.Tripathi Indian Institute of Information Technology,Allahabad," IMAGE COMPOSITE DETECTION USING CUSTOMIZED", International Journal of Computer Graphics & Animation (IJCGA) Vol.1, No.3, October 2011

[29] Jen-Chun Lee, Chien-Ping Chang, Wei-Kuei Chen," Detection of copy–move image forgery using histogram of orientated gradients," 2015, DOI: 10.1016/j.ins.2015.03.009

[30] Kavya Sharma," Computationally Efficient Copy-Move Image Forgery Detection Based on DCT and SVD," Advanced Research in Electrical and Electronic Engineering ,Volume 1, Number 3 (2014) pp. 76-81

[31] Kavya Sharma, Shweta Meena, UmeshGhanekar3," Hybrid Technique for Copy-Move Forgery Detection

Using L*A*B* Color Space," Int. Journal of Electrical & Electronics Engg.,Vol. 2, Spl. Issue 1 (2015) .

[32] Toqeer Mahmood, Tabassam Nawaz, Zahid Mehmood , Zakir Khan, Mohsin Shah, Rehan Ashraf," Forensic Analysis of Copy-Move Forgery in Digital Images Using the Stationary Wavelets," IEEE, pp576-583,2016.

[33] Jie Zhao, Jichang Guo," Passive forensics for copy-move image forgery using a method based on DCT and SVD," Forensic Science International 233 (2013) 158–166, DOI: 10.1016/j.forsciint.2013.09.013

[34] Singh, Vivek Kumar, and R. C. Tripathi. "Fast and efficient region duplication detection in digital images using sub-blocking method." international journal of advanced science and technology, Vol. 35, No. 1, pp. 93-102, 2011.

[35] Kodak dataset, Available: http://r0k.us/graphics/kodak/

[36] CoMoFoD dataset, Available: http://www.vcl.fer.hr/comofod/

[37] Columbia University dataset, Available: http://www.ee.columbia.edu/ln/dvmm/downloads/AuthSplicedDataSet/AuthSplicedData Set.htm

[38] CASIA dataset. Available: forensics.idealtest.org

[39] USC-SIPI dataset, Available: sipi.usc.edu/database

[40] HOG, Available: https://www.learnopencv.com/histogram-of-oriented-gradients/

[41] Nishmitha M.R and Aravind Naik," COMPARISON OF THREE TECHNIQUES OF IMAGE FORGERY DETECTION," International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) , Volume 14 Issue 2 –APRIL 2015

[42] Meera Mary Isaac, Dr. M. Wilscy," A Key point based Copy-Move Forgery Detection using HOG features,"IEEE,2016.

[43] GLCM,Available: https://www.ucalgary.ca/mhallbey/glcm1

[44] EXIFTool,Available: https://www.sno.phy.queensu.ca/~phil/exiftool/

[45] Jeffrey's Image metadata viewer, Available: http://exif.regex.info/exif.cgi

[46] EXIF-removal,Available: https://www.makeuseof.com/tag/3-ways-to-remove-exif-metadata-from-photos-and-why-you-might-want-to/

[47] Hex-editor,Available: https://en.wikipedia.org/wiki/Hex_editor

[48] Qazi, Tanzeela. "Survey on blind image forgery detection." IET , 2013.

[49] Ali Qureshi, M., and M. Deriche. "A review on copy move image forgery detection techniques." IEEE, 2014

[50] Huang, Hailing, Weiqiang Guo, and Yu Zhang. "Detection of copy-move forgery in digital images using SIFT algorithm." IEEE, 2008.

[51] Meera Mary Isaac, Dr. M. Wilscy," A Key point based Copy-Move Forgery Detection using HOG features," 2016 International Conference on Circuit, Power and Computing Technologies [ICCPCT],IEEE, 2016

Arun Anoop M obtained his BTech in Computer Science and Engineering from cochin university(College of Engineering, Thalassery, Kannur, Kerala(Under CAPE)). He completed his PG diploma in information security and system administration from DOEACC center, NIT , Calicut,Kerala and obtained his MTech in Information Technology from kalasalingam university, TamilNadu. Presently he is a PhD scholar under the supervision of Dr.S.Poonkuntran (Anna University, Chennai). His research center is Velammal College of Engineering & Technology, Viraganoor, Madurai, TamilNadu, India. He worked as an Assistant Professor in Computer Science and Engineering, MES College of Engineering, kuttippuram, kerala. Now he is on study leave for doing his FullTime PhD. Before joining MESCE he worked as teaching assistant in Information Technology, Kalasalingam university, krishnankoil, Tamilnadu. He is having 4 years of teaching experience at MESCE and 6months teaching experience at Kalasalingam University. He has attended 9 workshops, 4 FDPs. He served as a business development coordinator, Innoworld solutions, Pondicherry. His areas of interest are network security, Wireless Sensor Networks, digital forensics, Image Forensics, Multimedia security, Ethical Hacking. He has 12 International Journals. He has presented 12 International Conferences. He has presented 5 National conferences. He has written 3 books in Computer Science. He is a EC-Council certified Ethical Hacker v9 and Computer Hacking Forensics Investigator. He is a reviewer of IJCTT. He is hailing from Mattanur , Kannur (Dt.),Kerala.

Poonkuntran S. received B.E inInformation Technology from Bharathidasan University, Tiruchirapalli, India in 2003, M.Tech and Ph.D in Computer and Information Technology from Manonmaniam Sundaranar University, Tirunelveli, India in 2005 and 2011 respectively. He is presently working as a Professor and Head in Velammal College of Engineering and Technology, Madurai, Tamilnadu, India and executing three funded research grants from ISRO, India, DRDO, New Delhi and MNRE, New Delhi. He is having 12+ years of experience in teaching and research. He is a life time member of IACSIT, Singapore, CSI, India and ISTE, India. He has published papers in 4 national conferences, 38 international conferences, 1 national journal and 18 international journals on image processing, information security and soft computing. He has written 7 books in Computer Science. He was the State Level Student Coordinator Position for Region VII, CSI, India in 2016-17. Presently he is working on Computer Vision for under water autonomous vehicles and Information Security for Healthcare Information Systems. His areas of research interest include digital image processing, soft computing, energy aware computing and computer vision.