Detection of copy-move image forgery using Local Binary Pattern with Discrete wavelet transform and Principle Component Analysis

Mohanad Fadhil Jwaid
Department of Information Technology
Maharashtra Institute of Technology.Pune
Mohanad02jwaid@gmail.com

Prof. Trupti N. Baraskar
Department of Information Technology
Maharashtra Institute of Technology.Pune
Trupti.baraskar@mitpune.edu.in

Abstract

There has been a wide development in the zone of advanced picture usage. One of the fundamental problems in this present reality is to judge the genuineness of a particular picture. These days it is anything but difficult to alter and manufacture computerized picture with the progression of the capable advanced picture handling programming and simple accessibility of the apparatuses. The most widely recognized type of picture control systems is the district duplication additionally called as duplicate move falsification where a segment of the picture is replicated and glue to another part in the same advanced picture. To examine such legal investigation, different procedures and technique have been created in the past writing. In this paper will utilize productive calculations in light of Local Binary Pattern (LBP) with discrete wavelet transform (DWT) and principle component analysis (PCA). Firstly, change the picture from RGB to YCbCr by applying Pre-processing. Secondly, Discrete Wavelet Transform is applied above the image for compression. Guess sub-picture contains low recurrence parts having most extreme data. LL sub-picture is separated in covering squares. Thirdly Local Binary Pattern is performed. Fourthly principle component analysis is calculated for blocks to make descriptors to match related chunks as feature matching. The latest step is thru support vector machine (SVM) classify to choice which slice is the fake.

Keywords— Image forgery, Copy-Move Forgery, DWT, LBP, PCA, SVM.

I. INTRODUCTION

In advanced picture handling, picture fabrication is only the strategy of duplicating picture visual substance additionally altering utilizing the different distinctive picture investigations or altering instruments. Thus picture creativity and genuineness ends up noticeably significant risk in numerous constant applications like managing an account, news, legitimate handling records, wrongdoing examination, logical procedures and so forth [1]. Along these lines, such picture falsification may have come about into significant security danger as any end client can tamper or adjust the visual substance of unique picture without keeping any unmistakably known follows. There are diverse sorts of picture falsification like as picture joining, duplicate move and so forth. Mainly, Image fake is separated in two approaches. First one is an active approach where including digital watermarking and digital signature. A second approach is a passive approach where including copy-move image and splicing image. In this paper will base on the cope-move image. Image cloning forgery which is called as copy-move forgery is only one most risk full method of image fake, as user can able to modification full meaning of visual content of original image by copying some region from same or another image and pasted it on image part which is not necessary or to locate false information on original image by pasting it on original image part [2]. Principally, images with areas like gravel, grass, foliage, fabric etc. are best suitable to perform copy-move forgery due to fact that copied regions are possibly blended with an original image background and hence end users visually cannot able to maintain any suspicious artifacts by eyes.

Also, as photocopying is finished from a similar picture, its shading palette, clamor components, adaptable range, and other picture attributes are turned out to be good with different locales of unique computerized picture and subsequently not effectively identifiable with help of methods those are finding the inconsistencies amid the factual examination over different picture areas of picture. Editing or resizing is moreover utilized for having an effect of phony intense to find. Figure 1 indicates the case of duplicate move fraud [3]. In figure 1, it is demonstrating that the first confirmed picture of one flying creature on the left unique picture, in the correct fabrication picture we see two winged animals where replicated the flying creature from a unique picture and stuck in the second picture.

(a) (b)

Figure 1: Example of Copy-Move Forgery

Still, this category of forgery by visually is possible to track as copied and original regions of foliage are having suspicious similarity. There are different sorts of assaults happen amid imitation that is obscuring, scaling, commotion expansion, trimming, pressure, revolution, resizing, modifying, down examining, and so on. A number of mechanized strategies presented so far by a number of scientists for identify the picture imitation. Essentially duplicate move falsification comes about into the connection among unique picture district and produced picture area. Such relationship variable is used for precise distinguishing proof of such classification of fabrication [5] [6]. The distinguished districts of fabrication many not precisely situated because of sparing the picture in lossy JPEG arrange likewise utilization of various resizing, correct picture preparing instruments. In this way, underneath recorded are essential prerequisites for duplicate move imitation discovery: Algorithm for forgery detection must do the approximate matching of small regions of an image. An algorithm must work speedily with more accuracy and fewer errors. Forged region of an image must be represented in form of connected component rather than small pixels.

II. RELATED WORK

As of late, numerous inactive techniques for the discovery of Copy-move falsification have been genius postured. In the accompanying sections, we give an outline of the delegate strategies. We concentrate just on cutting-edge learning-based strategies. The fundamental separating component among these methods is the way, the auxiliary changes presented by altering are demonstrated.

In [7], the writer presented a matchless passive image fake discovery method is planned basis on (LBP) and (DCT) to discover copy-move & the splicing forgeries.

In [8], another technique for copy-move fake discovery newly presents in this article by the writer. This was different copy-move fake discovery method with adaptive over-division and feature point matching presented. This method combined both block-based and key points-based fake discovery schemes.

In [12], the methodology for copy-move forgery detection via the key points matching triangles was proposed. It is most different hybrid approach introduced by the author, this was very novel hybrid approach proposed by the author, which weigh triangles rather than blocks, or single points.

In [11], the author presented the procedure for copy-move forgery detection with aim of solving three existing problems.

In [10], this is another recent technique proposed for capable copy-move forgery detection on research public dataset images. The author presented this method for interest point detection is presented which was specialized for copy-move forgery detection. In this attitude, distribution of divided feature points reflects the local information content.

II. DISCRETE WAVELET TRANSFORM, LOCAL BINARY PATTERN AND PRINCIPLE COMPONENT ANALYSIS

This section explains the idea of techniques that used to discover copy-move forgery in this paper.

1 Discrete Wavelet Transform

DWT is a direct wavelet convert. It workings over vectors [5]. The length of vectors is regularly numbered differently of two which arranges information vector into unmistakable segments of recurrence. Pictures are disintegrated utilizing wavelets. Wavelet has an inbuilt multi-determination trademark [5]. DWT is connected over picture for the decay of picture which decreases picture estimate after each level of deterioration. The decay of a picture utilizing DWT is appeared in Figure (2). In two-dimensional DWT, DWT is connected to all lines than for all sections of a picture. If upload image is of size 2^nX2^n pixels at level L then after decomposition at level L+1 its size will be $2^{n/2}X2^{n/2}$pixels. When DWT is applied over an image, at each level image get decomposed in four sub-images. These sub-images also was known as sub-bands. Four sub-bands obtained after decomposition are LL, HL, LH and HH. When DWT is applied over an image, at each level image get decomposed in four sub-images. These sub-pictures otherwise called subgroups. Four sub groups gotten after disintegration are LL, HL, LH and HH. HH, LH, and HL sub-pictures contain slanting, the vertical and level segment of the picture, separately. LL is known as guess or coarse level sub-picture [5].

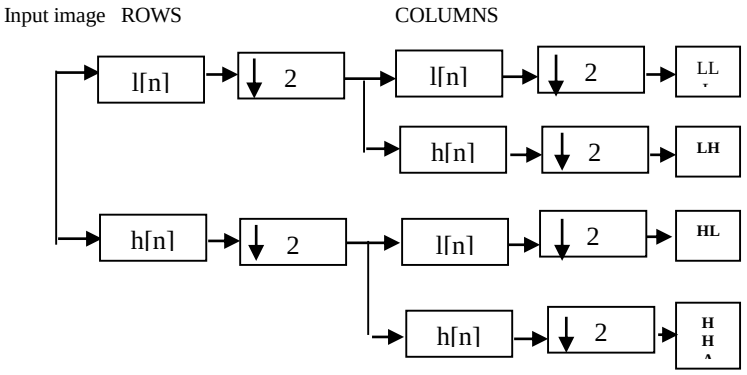

Figure 2: Image Decomposition using DWT[5]

2 Local Binary Pattern

Local Binary Pattern is a texture operator. It is useful in extricating dim level qualities. For ascertaining double examples a piece of the picture is considered for examination. Center value of pixel measured as the threshold as displayed in Figure (3). Neighbors hold value'1' if gray level values of neighbor pixels are greater than the threshold value. If gray level values of neighbor pixels are less than center value then the neighbor location of binary pattern holds value '0'. Advance, the same decimal value is considered for a binary pattern. Calculated decimal value is for center pixel. The Matching process is functional for wholly values of a chunk to compute LBP [6].

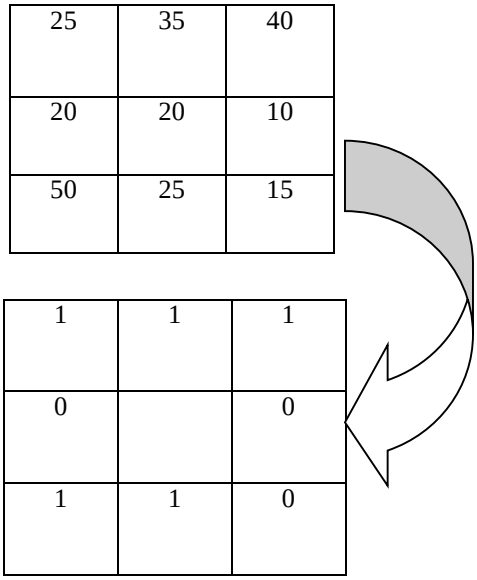

Figure 3: Calculation of Local Binary Pattern

3*3 block image

3 Principle Component Analysis

PCA is an awesome helpful channel in picture preparing. It is the most widely recognized and well known direct measurement lessening approach. It has been utilized for quite a long time as a result of it is theoretical effortlessness and calculation effectiveness [5].

III. PROPSED METHODOLGY

In this section, we projected a copy-move forgery detection methodology. Procedures of the proposed technique can be broadly distributed in four major steps which include image pre-processing, feature extraction, matching of similar chunks and grouping using SVM scheme. Initially, we upload one image called reference image as input and apply these steps, after this upload the second image called target image and repeat all these steps. The working flowchart representing the process of the proposed method is shown in figure (4).

1- Pre-processing :

In this step upload the reference image as the input image, the first part is converted image to gray scale image. The second part is extracting the R, G, B color (Red, Green, and Blue), then change it into YCbCr color (Luminance and Chrominance). The mathematical equation to convert RGB to YCbCr color are

Y=0.299R+0.587G+0.114B ..... (1)

Cr=0.701R−0.587G−0.114B..... (2)

Cb=−0.299R−0.587G+0.886B..... (3)

In this system to identify the forgery, we will base on CbCr (chrominance), because the human eye's sensitive is less than the Y (luminance). The chrominance space (CS) is calculated via subtracting luminance from red (Cr= R-Y) and via subtracting luminance from blue (Cb= B-Y). So the chrominance parts are employed to check whether the element extraction techniques are strategies are more touchy to altered pictures. These elements are used for applying Discrete Wavelet Transform over an image. Due to DWT image gets decomposed in four sub-bands LL, HL, LH, and HH. LL sub-band contain maximum information of an image. Hence, we selected it for further processing. As down sampling is used in DWT so image size get compact to 1/4 after each decomposition. Let input image is of size × B. Where K and B are number of rows and columns. Using DWT, its size reduced to≈ (K × B)/4[5]. In our method, image is divided in square blocks of dimension C × C. Total no. of square blocks are (K/ 2 − C + 1) ×(B/ 2 − C + 1).

2- feature extraction

In our scheme, texture operator (LBP) is operated for highlight extraction. For (K/ 2 − C + 1) × (B/ 2 − C + 1). A number of pieces, features are extracted. For each piece, components are put away in succession vector. All part vectors are secured in matrix$X$.Replicated and stuck pieces have same component vectors. To find relative pieces, we perceived same part vectors. In case component vectors are facilitated with each other for finding equivalence then the computational cost will be extensively high. For lessening organizing time, lexicographical sorting is associated over matrix$X$. This sorting framework achieves control of near part vectors in the neighborhood of each other and practically identical component vectors can be arranged in little scale go.

3- Feature Matching

PCA is working for matching. The sole purpose of feature matching is to discovery similar chunks of the image correctly. Matching is completed between feature vectors [10].

4- Classify

This is the latest step in our projected methodology. It is ended by consuming Support Vector Machine learning procedure(SVM).this technique is utilized after apply PCA matching, if the two images are not similar then the SVM is working to choice which slice is the fake by misleading the counterfeit part in the image[11].

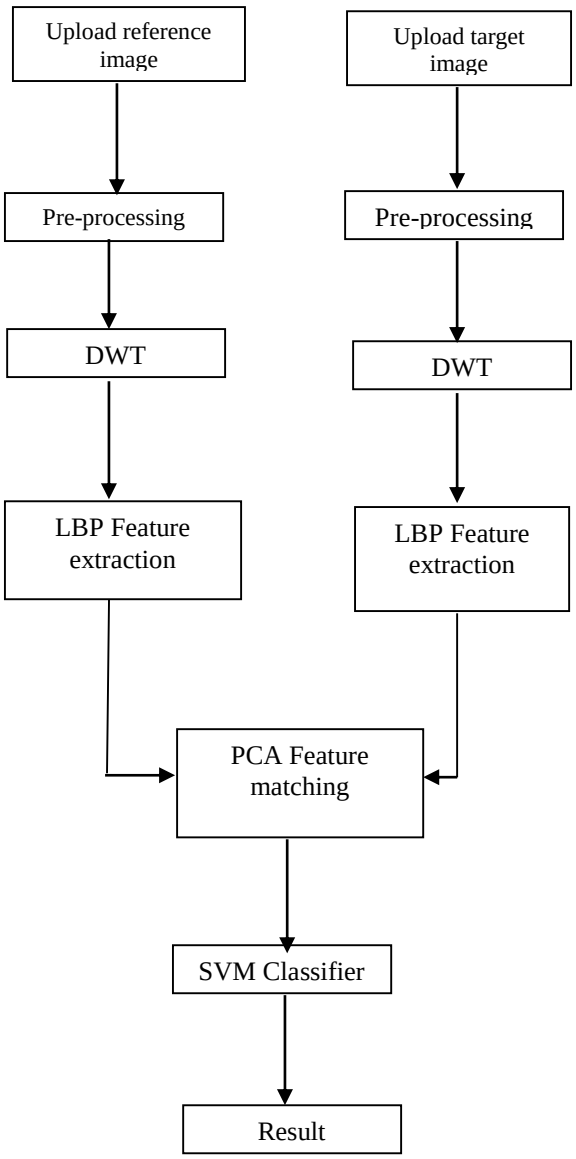

Figure 4: Block diagram of image forgery detection

IV. EXPERIMENTAL RESULT

In this division present the experimental outcome of our projected methodology to identify the copy-move image forgery. All the outcomes are executed on the engine with Intel Core i3, RAM 256 MB (min), with JAVA (jdk7) and Eclipse IDE. For investigating falsification comes about, pictures are taken from CoMoFoD database.

1- DATABASE

Copy-move forgery detection database (CoMoFoD) is involve of 260 forged image collections in two kinds (small 512x512, and large 3000x2000). Pictures are gathered in 5 bunches as indicated by connected control: interpretation, pivot, scaling, mix, and mutilation. Various kinds of post handling techniques, for the sample, JPEG pressure, obscuring, commotion including, shading diminishment and so forth, are linked to all produced and matchless pictures.

Table 1: CoMoFoD dataset

Category	Image category	Total number of images per category	Size of smallest copied area [pixels]	Size of biggest copied area [pixels]
Translation	512*512	40	360	28405
	3000*2000	10	7180	1130658
Rotation	512*512	40	403	37542
	3000*2000	10	11851	1040232
Scaling	512*512	40	403	37542
	3000*2000	10	11851	549188
Distortion	512*512	40	1037	37542
	3000*2000	10	24057	238083
Combination	512*512	40	403	37542
	3000*2000	10	6519	2611416

Table 2: The performance of dataset

	Dataset	**Accuracy %**
	CoMoFoD	**95.13**

2- Results

After complete registration in this system then logs into as a user, we upload the image to detect if it's original or forgery. Next figures show all steps with an image.

Figure 5: Original image

Figure 6: Forgery image

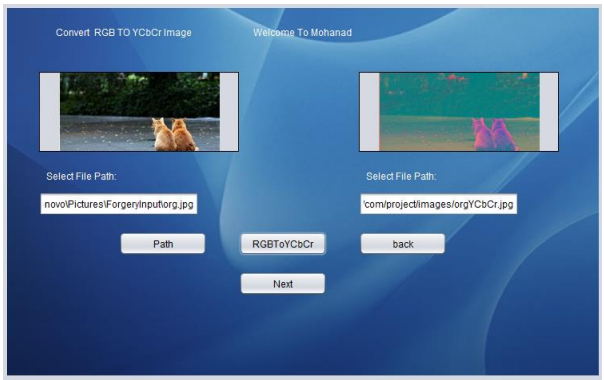

Figure 7: Pre-processing

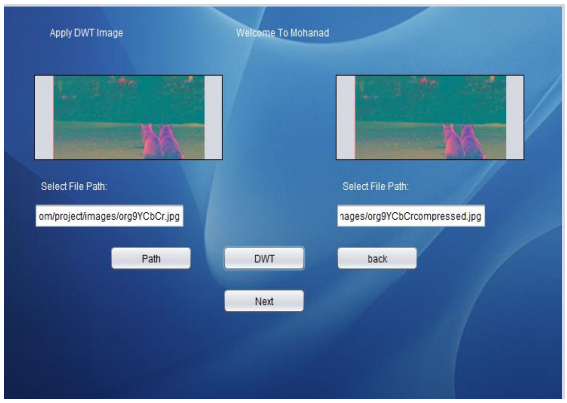

Figure 8: DWT

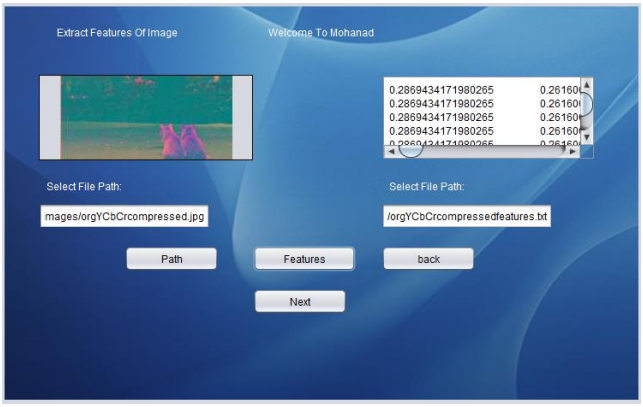

FIGURE 9: LBP FEATURE EXTRACTION

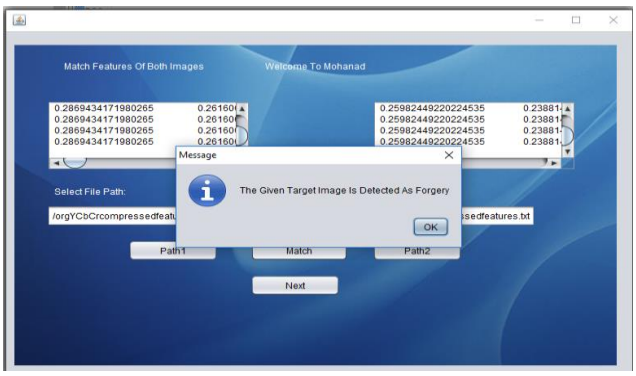

Figure 10: PCA matching feature

Figure 11: SVM classifier

Our parameters in this papers are detection accuracy (DA) and false match rate (FMR), where DA is the ratio of a number of forged pixels which are correctly matched to a number of actually forged pixels. And FMR is the ratio of a number of forged pixels which are falsely matched to a number of actually forged pixels. Table 3, 4 represents detection accuracy and false match rate of images. We observe here images with large size shows the highest value of detection accuracy and less number of false match rate. And the images with small size shows the highest number of a false match with a low value of detection accuracy. Proposed method can accurately detect forged areas. There are two kinds of size for the input image in this paper first one is small size including (90x90 and 90x120) pixels. Second one is large size including (140x200 and 160x260) pixels. The result will base over these two sizes wit parameters and divided input images into four kinds if block size including (11x11, 15x15, 19x19 and 23x23) pixels.

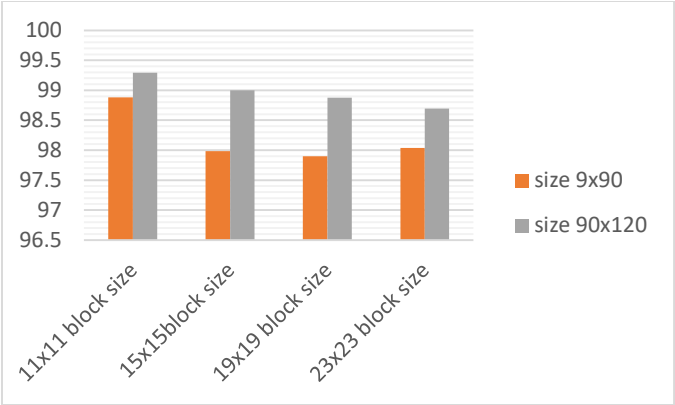

Figure 12: Detection Accuracy for small image forgery detection

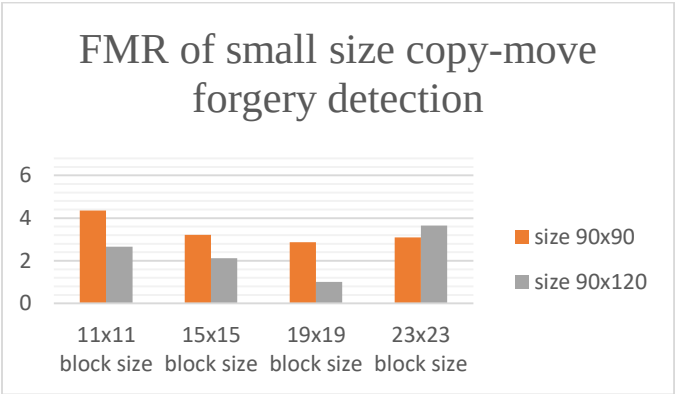

Figure 13: False match rate for small image forgery detection

Table (3): DA and FMR values of small size copy-move forgery image

Block size of input image (pixel)	DA%		FMR%	
	90x90 Image size	90x120 image size	90x60 Image size	90x120 image size
11x11	98.8826	99.2912	4.3570	2.6521
15x15	97.9828	98.9981	3.2070	2.1260
19x19	97.9012	98.8772	2.8675	1.0103
23x23	98.035	98.6921	3.0981	3.6482

Table (4): DA and FMR values of large size copy-move forgery image

Block size of input image (pixel)	DA%		FMR%	
	140x200 Image size	160x260 image size	140x200 Image size	160x260 image size
11x11	99.2821	99.7241	2.9812	1.8821
15x15	99.5637	99.7671	1.502	0.1981
19x19	97.9821	98.7512	2.5412	0.5213
23x23	98.1361	98.9.33	3.0123	2.1006

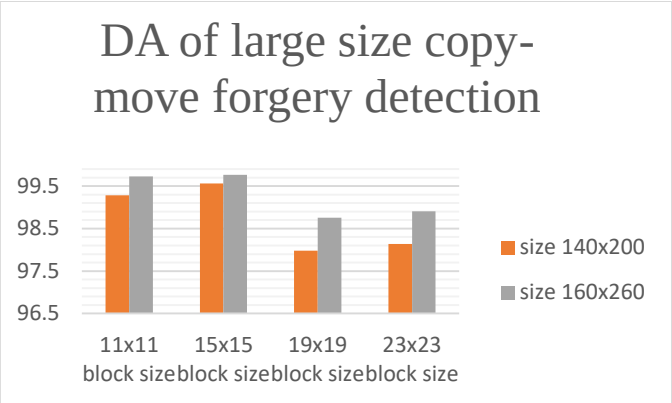

Figure 14: Detection Accuracy for large size image forgery detection

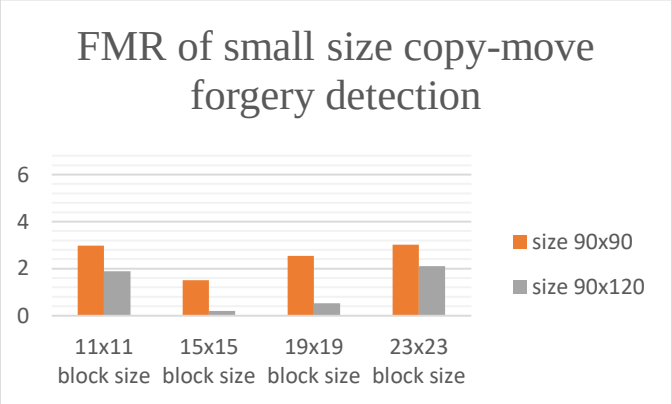

Figure 15: False match rate for large size image forgery detection

Conclusion

In this paper presented the meaning of copy-move forgery image, and how can we detect the forgery by designing a system based on efficient techniques including DWT for compression, and LBP for feature extraction then apply PCA for feature matching and last one is SVM classifier. The result is achieved by 99 %. The next work will make this system applicable to the large size of images.

REFERENCES

[1] Jessica F, David S, and Jan L, "Detection of copy-move forgery in digital images," in in Proceedings of Digital Forensic Research Workshop, 2003".

[2] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515, 2004".

[3] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An Evaluation of Popular Copy-Move Forgery Detection Approaches," Ieee Transactions on Information Forensics and Security, vol. 7, pp. 1841-1854, Dec 2012".

[4] R. Achanta, A. Shaji, K. Smith, A. Lucchi, P. Fua, and S. Susstrunk, "SLIC superpixels compared to state-of-the-art superpixel methods," IEEE Trans Pattern Anal Mach Intell, vol. 34, pp. 2274-82, Nov 2012".

[5] Fahim Hakimi, Mahdi Hariri, Farhad GharehBaghi, "Image Splicing Forgery Detection using Local Binary Pattern and Discrete Wavelet Transform", 2nd international conference on KBEI, IEEE, 2015".

[6] Diaa M. Uliyan, Hamid A. Jalab, Ainuddin W. Abdul Wahab, "Copy Move Image Forgery Detection Using Hessian and Center Symmetric Local Binary Pattern", 2015 IEEE Conference on ICOS, 2015".

[7] Amani Ahmadi, Muhammad Hussain, Hatim Aboalsamh, Ghulam Muhammad, George Bebis, Hassan Mathkour, "Passive Detection of Image Forgery using DCT and Local Binary Pattern", Signal Image and Video Processing • April 2016".

[8] Chi-Man Pun, Xiao-Chen Yuan, Xiu-Li Bi, "Image Forgery Detection Using Adaptive Over-Segmentation and Feature Point Matching", IEEE Transactions on Information Forensics and Security, 2015".

[9] Khosro Bahrami, Alex C. Kot, Li, and Haoliang Li, "Blurred Image Splicing Localization by Exposing Blur Type Inconsistency', IEEE Transactions on Information Forensics and Security, 2015".

[10] Mohsen Zandi, Ahmad Mahmoudi-Aznaveh, and Alireza Talebpour, "Iterative Copy-Move Forgery Detection based on a New Interest Point Detector", IEEE Transactions on Information Forensics and Security, 2016".

[11] Anselmo Ferreira, Giovanni C. Felipe's, Carlos Alfaro, "Behavior Knowledge Space-Based Fusion for Copy-Move Forgery Detection", TRANSACTIONS ON IMAGE PROCESSING, 2016".

[12] E. Ardizzone, A. Bruno, and G. Mazzola, "Copy-Move Forgery Detection by Matching Triangles of Keypoints", IEEE Transactions on Information Forensics and Security, 2015".