Proposed Novel Method of Image Forgery Detection Using DWT Transform Function Using Genetic Algorithm

Reshu tamrakar
M.Tech Scholar, Department of CSE
PIES, Bhopal INDIA
E-mail- reshu.tamrakar@gmail.com

Prof. Pankaj Kawadkar
Department of CSE
PIES, Bhopal India
E-mail:-kawadkarpankaj@gmail.com

ABSTRACT
In current decade, digital images are in use in a wide range of applications and for multiple purposes. They also play an important role in the storage and transfer of visual information, especially the secret ones. With this widespread usage of digital images, in addition to the increasing number of tools and software of digital images editing, it has become easy to manipulate and change the actual information of the image. Therefore, it has become necessary to check the authenticity and the integrity of the image by using modern and digital techniques, which contribute to analysis and understanding of the images' content, and then make sure of their integrity. In this detection technique used texture feature of image. For the texture extraction of image used wavelet transform function, these function is most promising texture analysis feature. For the selection of feature generation of pattern used clustering technique. Clustering technique is unsupervised learning technique process by iteration. The proposed methods are evaluated on a number of original and forged images. According to our experimental results the proposed methods are quite attractive. The forgery is done with just copy-move, copy-move with rotation, with scaling, and reflection. In this process, an image database that consists of original and forged images is also developed. The proposed method achieves 100% accuracy in just copy-move forgery (without any change in the size or characteristics of the object) forgery without post-processing and 98.43%, 86.58%, and 95.12% accuracies in copy-move forgery with rotation, scaling, and reflection, respectively.

Index Terms:- Image forgery, Classification, DWT, K-Means.

INTRODUCTION

Forgeries are not new to mankind but are a very old problem. In the past it was limited to art and literature but did not affect the general public. Nowadays, due to the advancement of digital image processing soft-ware and editing tools, an image can be easily manipulated and modified. Digital images in the current era play very important role in various fields. They are used in different applications in the area of military, news, medical diagnosis and media, to mention a few. Due to the development in technology of digital image, for example, cameras, software, and computers and the wide spread via the internet, digital image can be considered a major source of information in today's digital world. But to believe what we see, we must make sure that the image is original. Thus the images are required to pass the test authenticity. It is very difficult for humans to identify visually whether the image is original or manipulated. There is rapid increase in digitally manipulated forgeries in mainstream media and on the Internet [4]. This trend indicates serious vulnerabilities and decreases the credibility of digital images. Therefore, developing techniques to verify the integrity and authenticity of the digital images is very important, especially considering that the images are presented as evidence in a court of law, as news items, as a part of medical records, or as financial documents. In this sense, image forgery detection is one of the primary goals of image forensics.

Verifying the integrity of digital images and detecting the traces of tampering without using any protecting pre-extracted or pre-embedded information have become an important and hot research field of image processing. In our society digital images has significant role in every-one's lives, which are widely used in medium of communication, forensic investigations, insurance processing, surveillance systems, intelligence services, medical imaging and political campaigns [10]. A digital image can be retouched or maliciously tampered with ease, and the information in which could be altered without leaving any obvious trace with the help of a sophisticated photo editor. Region duplication is a kind of tampering commonly seen in digital image forgery. The sub-area of an image is copied and pasted to another location of this image, to conceal or duplicate the interested object in the image. The two forgeries are image inpainting and copy paste forgery. Image inpainting is a technique to reconstruct portion of the image which has been removed using the information from the rest of the image. Exemplar-based image inpainting is currently state of the art for Image Inpainting. Object removal and region filling by image inpainting is significant for content correction by removing unwanted objects and for image restoration by repairing damaged portions. It is also a tool for photo-montages leading to privacy violation and cybercrimes. It thus requires for the development of a forensic technique to detect forged

inpainted images. On the other hand a copy move forgery is one in which a part of the image itself is copied and pasted into another place in the same image. It is also known as cloning. Textured regions such as foliage, grass, gravel or irregularly patterned fabrics are ideal for this purpose because the copied areas will probably blend with the background. Thus it makes it difficult for human discern any suspicious artifacts.

Digital image forgery detection techniques are classified into active and passive approaches. In active approach, the digital image requires some pre-processing such as watermark embedding or signature generation at the time of creating the image, which would limit their application in practice. Moreover, there are millions of digital images in internet without digital signature or watermark. In such scenario active approach could not be used to find the authentication of the image [15]. Unlike the watermark-based and signature-based methods; the passive technology does not need any digital signature generated or watermark embedded in advance.

II DETECTION OF COPY/MOVE FORGERY

In a Copy-Move forgery, a part of the image itself is copied and pasted into another part of the same image. This is usually performed with the intention to make an object "disappear" from the image by covering it with a segment copied from another part of the image. Textured areas, such as grass, foliage, gravel, or fabric with irregular patterns, are ideal for this purpose because the copied areas will likely blend with the background and the human eye cannot easily discern any suspicious artifacts. Because the copied parts come from the same image, its noise component, color palette, dynamic range, and most other important properties will be compatible with the rest of the image and thus will not be detectable using methods that look for incompatibilities in statistical measures in different parts of the image. To make the forgery even harder to detect, one can use the feathered crop or the retouch tool to further mask any traces of the copied-and-moved segments. It is one of the most popular forms of tampering in which some region is copied from a particular location in an image and thereafter pasted at one or more locations within the same image or a different image of preferably the same scene . Two examples are given in below Figure to demonstrate the copy/move forgery. The original image, as reported in in the form of below Figure, is depicting two army vehicles. The truck has been camouflaged from the image by copying a region that is roughly of a circumference as indicated by the circle and moved to the location of the truck (in the original image).

IMAGE RETOUCHING

Image retouching is another class of forensic methods that pertains to a slight change in the image for various aesthetic and commercial purposes, not necessarily conforming to the standards of morality. The retouching is mostly used to enhance or reduce the image features. Usually this type of forgery is realized by changing the color or texture of the objects, intensify the weather conditions or simply introducing some blur for defusing the objects. The example demonstrates the effects of the retouching. Below figure left one is the original image, whereas right side image shows the change of colors of the headlights and some background objects. Image retouching has long been the norm in commercial photography, usually for photo-sessions, as well as a routine in the showbiz industry. This type of forgery is also known as the image enhancement for its use to improve facial features.

III PROBLEM STATEMENT

In this section discuss some common problem related to image forgery detection some are discuss below:

1. **Data Provenance**

The data provenance is necessary for protection of rights and may be regulatory requirement in applications like science, medicine, financial transactions government legal prosecutions and many more daily situations, wherever the information is valuable and trustworthy.

2. **Benchmarking and Standard data set**

There is need of open data sets for critical and typical realistic conditions such as images (digital documents) in uncompressed form with different resolutions, sizes and image acquisition model (camera model) with diverse contents for all possible forgeries such as copy-move, compositing, splicing, photomontage, blending, matting etc. with manipulation, and manipulation compensation conditions like adjustments color, contrast, brightness, blurring, enhancement and possible post suppression

3. **Duplicate Regions**

The reason of the appearance of duplicate regions in an image is one of two things: first, the presence of two things or two objects with the same size, shape, and color; one of them may be a copy from the other one. Second, the presence of a relatively large area with one color and close in characteristics such as backgrounds (sky, wall, etc.) which leads to the appearance of duplicate regions in the results.

IV PROPOSED WORK

In this section discuss the proposed algorithm for image forgery detection based on clustering technique. In the process of image forgery k-means clustering technique is applied. The k-means clustering technique is very efficient for the creation of block pattern. After the creation of block pattern used block matching process. For the purpose of clustering used texture feature data for forged and original image.

In this section describe the process of proposed model. The proposed model contain with wavelet transform function and clustering technique. The clustering technique generates the local pattern of block.

Step 1. Initially put the original image and forged image for the processing of feature extraction

Step 2. After processing of image discrete wavelet transform function are applied for the texture feature extraction

Step 3. After the texture feature extraction apply k-means technique for local pattern generation

Step 4. The pattern matching block selects the all local pattern of cluster algorithm of both original and forged image

Step 5. Measure the distance between original image and forged image.

Step 7. If the value of d is 0 images are block is original else image block area is forged.

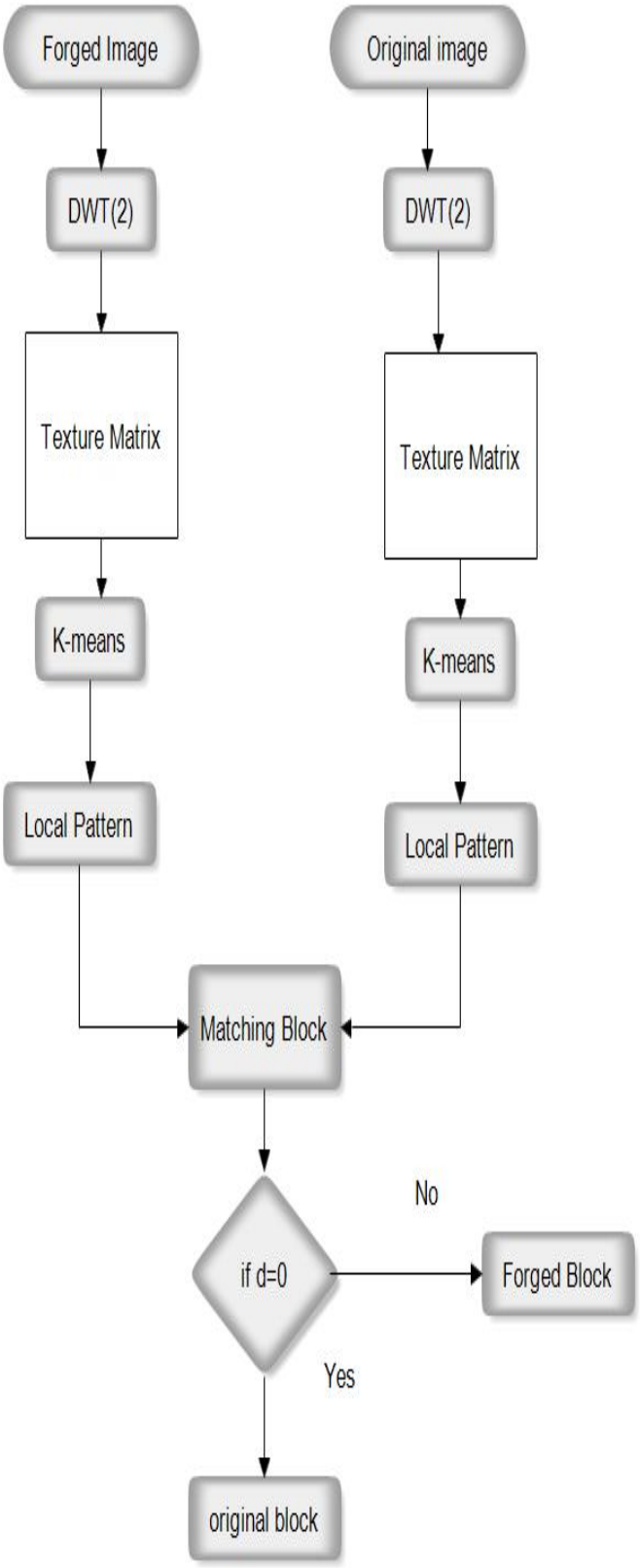

Figure 1: proposed model for image forged image

V RESULT ANALYSIS

It is simulating on mat lab 7.14.0 and for this work we use Intel 1.4 GHz Machine. MATLAB is a high level technical computing language and interactive environment for algorithm development, data visualization, data analysis, and numeric computation Mat lab is a software program that allows you to do data manipulation and visualization, calculations, math and programming.

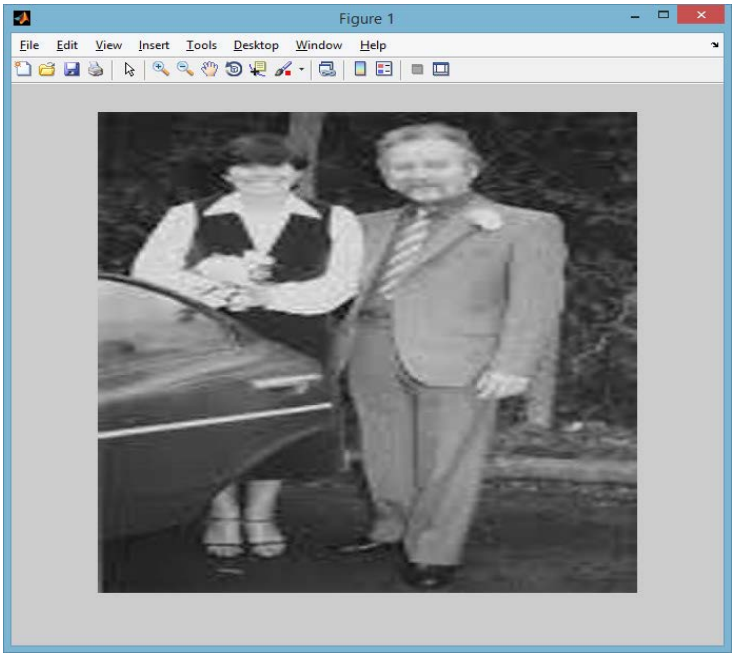

Figure 2: Shows that the images load initially from the dataset.

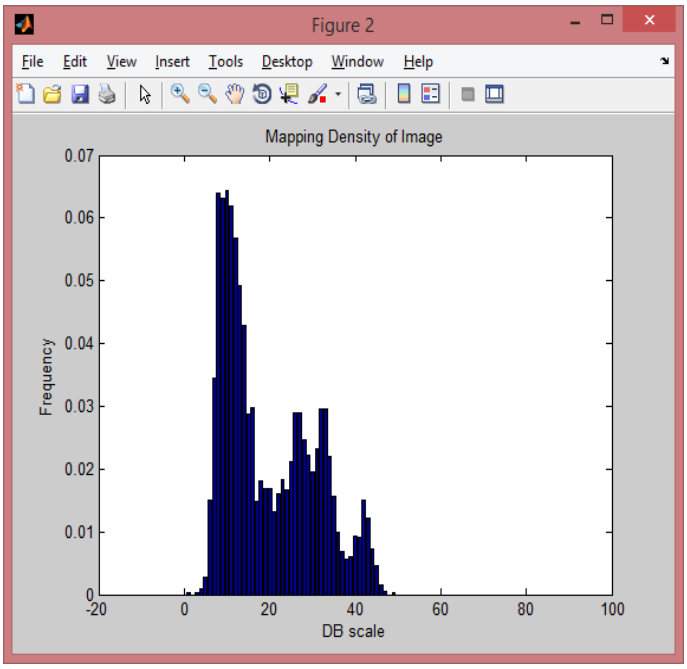

Figure 3: Mapping Density of Image1.

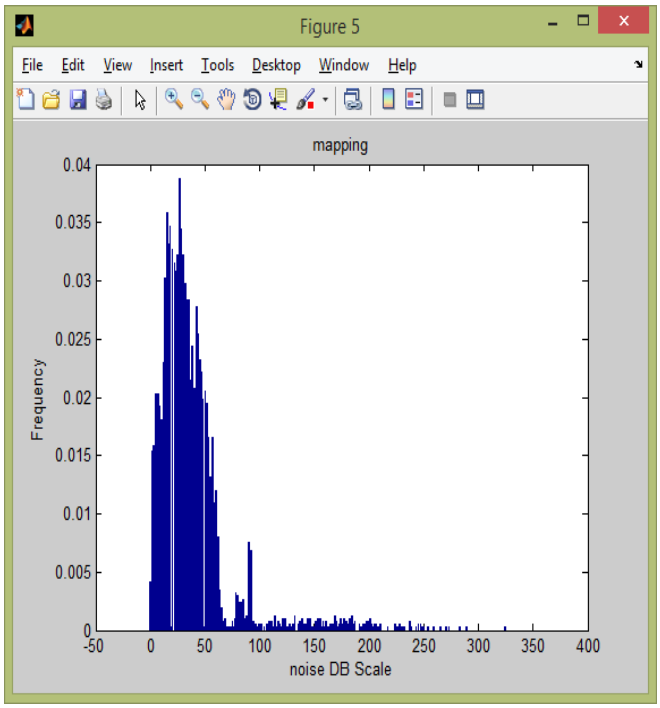

Figure 4: Mapping of Forest image for the proposed technique.

Image name	Method	Detection Rate In %	FRR In %
Couple	LDBM	87.79	2.10
	PROPOSED	93.82	.420
Forest	LDBM	88.12	1.93
	PROPOSED	94.12	.268
Historical	LDBM	86.24	3.18
	PROPOSED	92.67	1.48
Water Fall	LDBM	89.27	3.820
	PROPOSED	95.48	.987

Table 1: Shows that the Detection Rate and FRR with using LDBM and Proposed method for the same and different number of images.

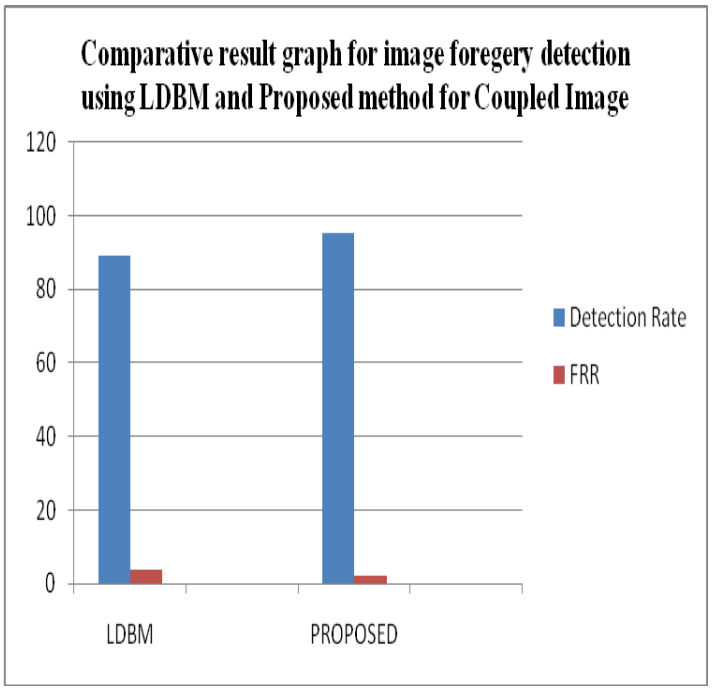

Figure 5: Shows that comparative result of Image "Coupled", with using LDBM and Proposed method and here our proposed method shows that the better result in the form of higher Detection Rate and low FRR than the existing method.

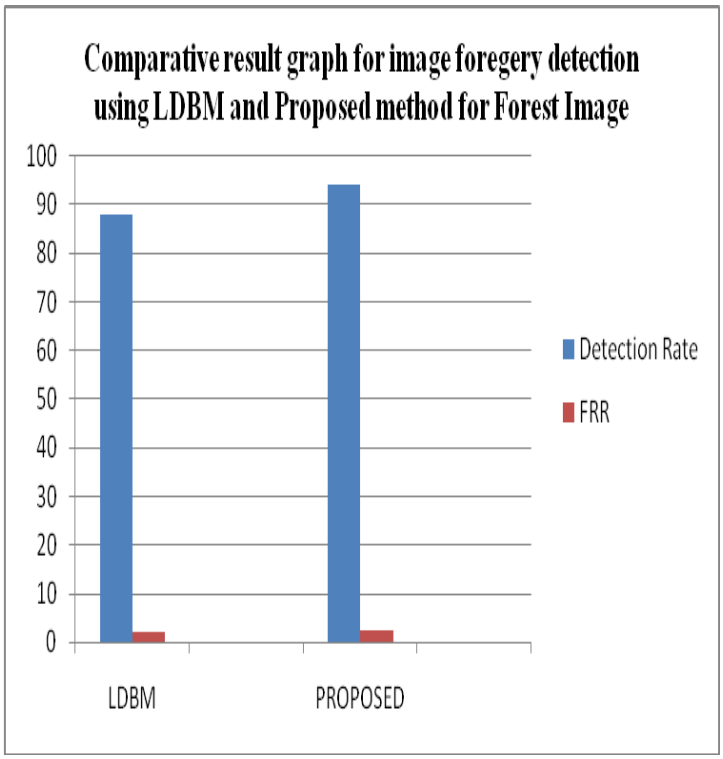

Figure 6: Shows that comparative result of Image "Forest", with using LDBM and Proposed method and here our proposed method shows that the better result in the form of higher Detection Rate and low FRR than the existing method.

VI CONCLUSION

In this paper proposed an image forgery detection technique based on clustering technique. The proposed image forgery used wavelet transform function for the extraction of feature of original and forged image. The extracted feature passes through clustering technique for the generation of local pattern. The local pattern passes though matching block and measure distance of two similar and dissimilar blocks. The proposed image forged detection technique is very efficient in compression of local pattern and transform function based technique.

The proposed methods are evaluated on a number of original and forged images. According to our experimental results the proposed methods are quite attractive. The forgery is done with just copy-move, copy-move with rotation, with scaling, and reflection. In this process, an image database that consists of original and forged images is also developed. The proposed method achieves 100% accuracy in just copy-move forgery (without any change in the size or characteristics of the object) forgery without post-processing and 97.43%, 66.58%, and 99.12% accuracies in copy-move forgery with rotation, scaling, and reflection, respectively. Also to ensure more efficiency, we have added some random noise on the images, the detection accuracy achieved 98.23%. While the proposed method performs well even with additive white Gaussian noise post-processing. For the evaluation of performance of copy-move forgery detection in digital images, in future, we commend the following improvements.

a. Some sophisticated constraints on the feature selector genetic can be applied to make the system more robust.
b. Detecting small target area and big size image using optimization technique.
c. Applying different classification technique for pattern generation process.

REFERENCES:-

[1] Giovanni Chierchia, Giovanni Poggi, Carlo Sansone, Luisa Verdoliva “A Bayesian-MRF Approach for PRNU-Based Image Forgery Detection” IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, Vol-9, 2014. Pp 554-567.

[2] Andrea Costanzo, Irene Amerini, Roberto Caldelli, Mauro Barni “Forensic Analysis of SIFT Keypoint Removal and Injection” EEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, Vol-9, 2014. Pp 1450-1464.

[3] Neenu H.U., Jini Cheriyan “Image Forgery Detection based on Illumination Inconsistencies & Intrinsic Resampling Properties” International Conference on Magnetics, Machines & Drives, IEEE 2014. Pp 1-6.

[4] Ghulam Muhammad, M. Solaiman Dewan, M. Moniruzzaman, Muhammad Hussain, M. Nurul Huda “IMAGE FORGERY DETECTION USING GABOR FILTERS AND DCT” International Conference on Electrical Engineering and Information & Communication Technology, IEEE, 2014. Pp 254-259.

[5] Davide Cozzolino, Diego Gragnaniello, Luisa Verdoliva “MAGE FORGERY DETECTION THROUGH RESIDUAL-BASED LOCAL DESCRIPTORS AND BLOCK-MATCHING” IEEE, 2014. Pp 5297-5302.

[6] Abhishek Kashyap, Shiv Dutt Joshi, “Detection of Copy-Move Forgery Using Wavelet Decomposition” IEEE, 2013, Pp 396-400.

[7] Saba Mushtaq and Ajaz Hussain Mir, “Digital Image Forgeries and Passive Image Authentication Techniques: A Survey” International Journal of Advanced Science and Technology (IJAST), 2014, Vol.73, Pp 15-32.

[8] Ketan S Bacchuwar, Aakashdeep, K.R Ramakrishnan, “A Jump Patch-Block Match Algorithm for Multiple Forgery Detection” IEEE, 2013, Pp 723-726.

[9] Ghulam Muhammada, Muhammad Hussain , George Bebis , “Passive Copy Move Image Forgery Detection using Undecimated Dyadic Wavelet Transform” Digital Investigation, 2012,Vol. 9,Pp 49-57.

[10] Sondos M. Fadl , Noura A. Semary, Mohiy M. Hadhoud, “Copy-Rotate-Move Forgery Detection Based on Spatial Domain” IEEE,2014,Pp 136-141.

[11] Cheng-Shian Lin and Jyh-Jong Tsay, ” Passive Forgery Detection for JPEG Compressed Image based on Block Size Estimation and Consistency Analysis” Natural Science Publishing Cor.,2015, Pp 1015-1028.

[12] Michael Zimba,Sun Xingming, “DWT-PCA (EVD) Based Copy-move Image Forgery Detection” IJDCTA, Vol.5, 2011, Pp 251-258 .

[13] Ghulam Muhammad , Munner H, Al-Hammadi , Muhammad Hussain, George Bebis , “Image Forgery Detection using Steerable Pyramid Transform and Local Binary Pattern” Springer-Verlag Berlin Heidelberg ,2013.

[14] Tiziano Bianchi, Alessia De Rosa, Alessandro Piva, “ Improved DCT Coefficient Analysis For Forgery Localization In JPEG Images” IEEE, 2011. Pp 2444-2447.

[15] H. Farid, "Image Forgery Detection" Signal Processing Magazine, IEEE, March 2009,Vol. 26, No. 2, Pp 16-25.

[16] G. Cao, Y. Zhao, R. Ni and X. Li, “Contrast Enhancement-Based Forensics in Digital Images” IEEE Transactions on Information Forensics and Security, 2014,Vol 9, No. 3, Pp 515-525.

[17] G. Chierchia, G. Poggi, C. Sansone and L. Verdoliva, “A Bayesian-MRF Approach for PRNU-Based Image Forgery Detection” Information Forensics and Security, IEEE Transactions, 2014, Vol. 9, No. 4, Pp 554-567.

[18] G. K. Birajdar and V. H. Mankar, “Digital Image Forgery Detection using Passive Techniques: A survey” Digital investigations, 2013, Pp. 226-245.

[19] P. Xunyu and L. Siwei, "Region Duplication Detection using Image Feature Matching", IEEE Trans on Information Forensics and Security, 2011, Vol. 5, No. 4, Pp 857–67.

[20] P. Kakar and N. Sudha, "Exposing Post Processed Copy-paste Forgeries through Transform-invariant Features", IEEE Trans. on Information Forensics and Security, 2012, Vol. 7, No. 3,Pp 1018–28.