An Eficient Approach to Copy Move Forgery Detection using DWT and SIFT Features

Ms. Apeksha Ingle[1], Prof. (Dr.) C. N. Deshmukh[2], Prof. (Dr.) D. T. Ingole[3]
[1]*ME Scholar, PRMIT&R, Badnera*
[2]*Head Dept. of CSE-IOT, PRMIT&R, Badnera*
[3]*Principal, KGIET, Darapur*

***Abstract*—The topic of copy move forgeries is becoming more and more popular among picture forensic experts. Essentially, copy move forgery involves replicating a single area in a picture by pasting a specific section of the same image onto it. Several methods have been employed to identify this kind of counterfeit. An improved method for identifying copy move forgeries is put forth in this research. To improve the robustness and accuracy of copy-move forgery detection, the suggested approach combines block-based techniques like Discrete Wavelet Transform (DWT) with feature-based techniques like Scale Invariant Feature Transform (SIFT). Initially, a picture is subjected to DWT in order to deconstruct it into four parts: LL, HL, HH, and LH. Since the majority of the information is contained in the LL component, SIFT is only applied to the LL part in order to further extract the image's essential features, match those features using interblock matching, identify the identical portion or portions between the images, and designate them as forged. This technique more precisely highlights the fraud and determines whether picture forgery has happened.**

I. INTRODUCTION

In today's technologically advanced society, "seeing is no longer believing."The majority of the information is transmitted digitally, particularly as digital photos or movies. As a result, they comprise the information carrier's main stream. It is incredibly easy to manipulate these sources. Image counterfeiting, which has grown to be a significant concern, will be the main topic of this essay. Any given image can be easily altered with the help of widely accessible image editing software like Adobe Photoshop. This can have major repercussions because tampered images may be used as evidence in court, which could result in an incorrect decision and false beliefs in many real-world applications. As a result, the matter of image authentication needs to be handled with extreme caution. As illustrated in Fig. 1, the majority of forgery detection methods fall into one of two basic categories: intrusive/non-blind and non-intrusive/blind [1].

The intrusive approach, often referred to as a non-blind method, has a limited scope because it necessitates that some digital information be implanted in the original image at the time of generation. Watermarking and employing the camera's digital signature are two examples of these techniques, yet not all digital gadgets have this capability.

However, no embedded information is needed for the non-intrusive approach, also referred to as the blind method. When an original digital image is altered by performing different transformations, such as rotation, scaling, resizing, etc., it is considered to be forged [6]. In order to conceal the true information, an image may also be altered by adding noise or by deleting or adding objects.

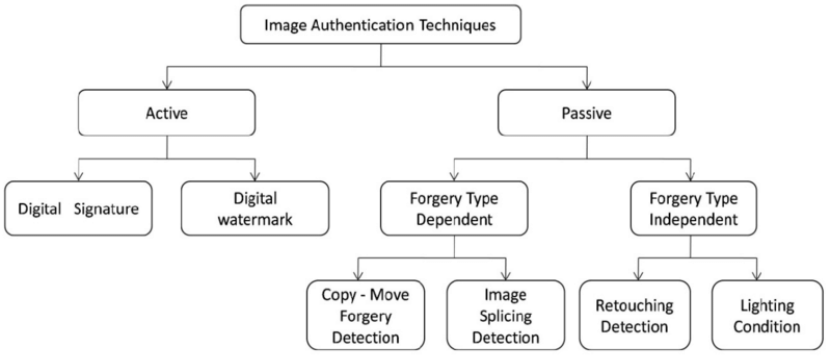

Fig.1. Classification of image forgery detection technique

II. RELATED WORK

After reviewing several blind techniques for detecting copy-move picture forgeries, Saika et al. [1] proposed a blind and reliable method that makes use of the discrete wavelet transform (DWT).Sunil Kumar et al. [2] talked about techniques that lessen the total computational load, The provided image was first broken down into four distinct sub-bands, LL, LH, HL, and HH, using DCT. Since the low frequency band contains the majority of the information, the low frequency sub-band, or LL band, is separated into overlapping blocks. H. Huang et al. [6] represented the features of the provided image using the SIFT technique.The SIFT method remains unaffected by variations in lighting, rotation, scale, and other factors. N. Anantharaj [7] discusses utilizing Scale Invariant Features Transform (SIFT) to determine whether or not an image has been forged, particularly when copymove forgery is involved. SIFT recovers from the geometric transformation employed for cloning and enables the understanding of copy-move forgeries. We can also address multiple copy-move forgery with this technique. In order to identify copy-move image counterfeiting, Amanpreet Kaur et al. [11] developed a method that combines DCT and SIFT. A overview of copy move forgery detection methods on digital photographs was presented by Salam A. Thajeel [12]. In order to identify the forged sections, Rohini A. Maind [13] suggested an effective technique that uses local binary patterns. The image is first filtered and then separated into overlapping circular blocks, and the features of these blocks are computed using local binary patterns. Popescu et al. [14] provided further recommendations for future research in addition to summarizing a thorough exposure of digital forgeries by identifying duplicated image portions. A copy-move forgery image forensics investigation was presented by Nandini Singhal et al. [15]. An method was presented by Vincent Christlein et al. [16] for assessing copy-move forgery detection techniques.

III. METHODOLOGY

The idea behind this paper is to use digital images to detect malicious manipulation. In order to extract SIFT features, the input image is first broken down using one of the DWT bases functions. Matching is done among the clusters and then the out liners are deleted to produce the final detection result.

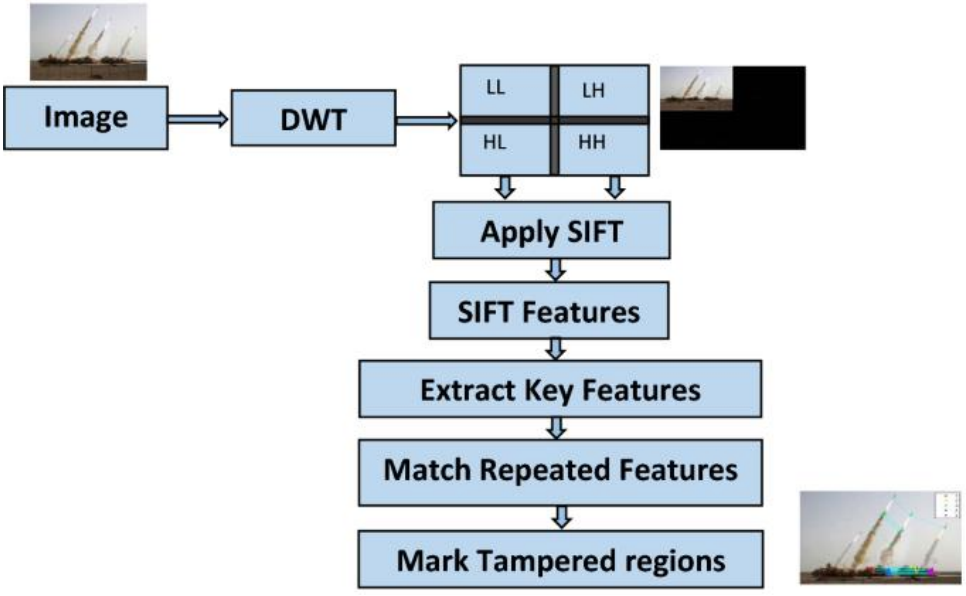

Fig.2: The Pretrained ALEXNET process

IV. SYSTEM DEVELOPMENT AND EXPERIMENTAL RESULTS

4.1 System Development

For demonstration of proposed system, graphical user interface is developed as shown in Fig 3 . It consists of pushbutton ‘Select the Image’ and two windows namely ‘Input Image’ and ‘Result’.

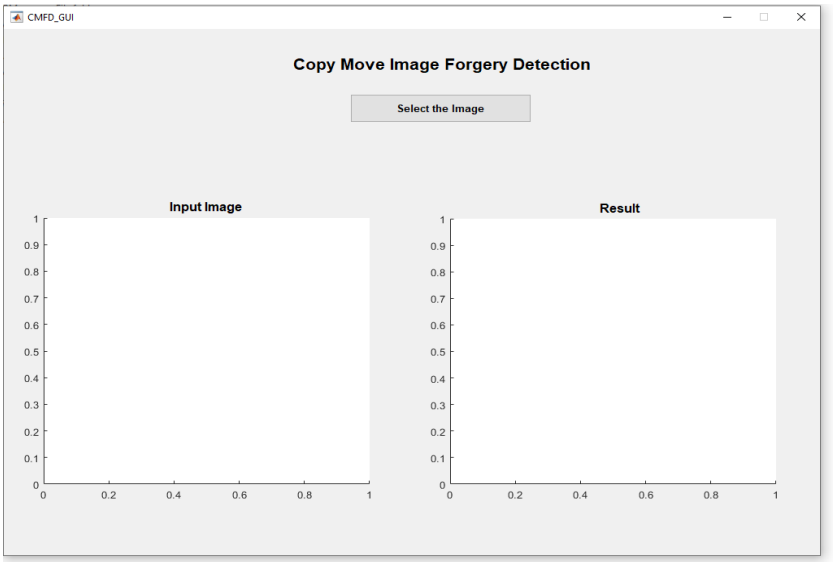

Fig. 3 GUI of proposed system

On clicking 'Select the Image', the GUI prompts for new window for browsing and selection of query image. After selction of the query image, the process started and the result is calculated as shown in Fig. 4 where red boundary is used to mark the forged region. If the image is not forged then "Image is Original" is indicated by the system as shown in Fig. 5

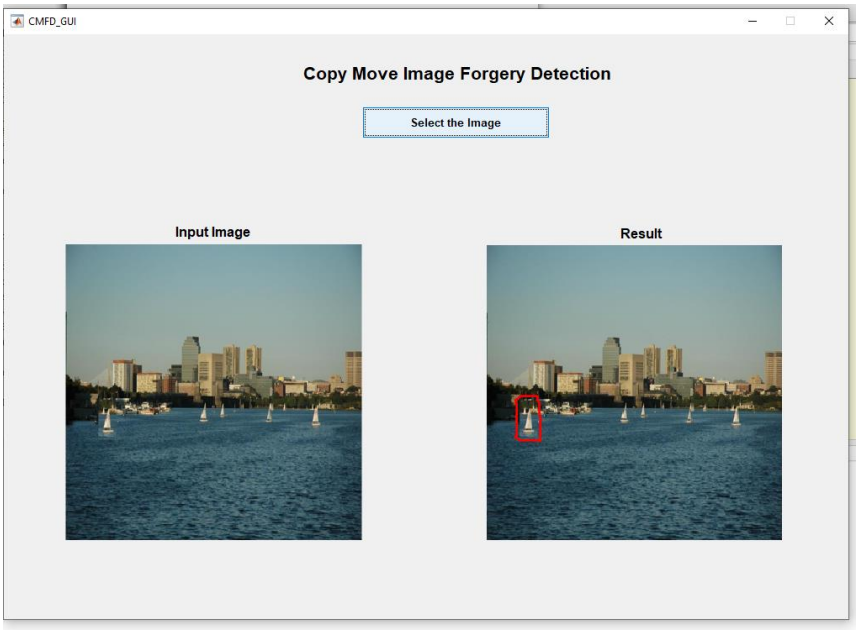

Fig. 4 Result of the proposed method

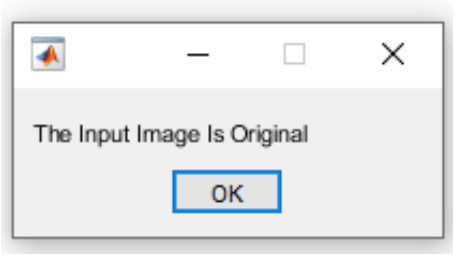

Fig. 5 Result for Non-forged image

4.2 Experimental Results

The standard database is used for experimentation of the proposed method. The database considered is MICC F220 and MICC F2000. These datasets consist of 220 and 2000 images respectively. They build their forged images by randomly copying the location and the dimension of a square or rectangular area from the image and pasting the shape over the same image. Different types of transformation have been applied to the forged images, such as translation, rotation, scaling or combination [7].

For detailed understanding of the processes involved in the complete experimentation, one sample image is taken into consideration and steps explained.

Fig. 6 Sample image 2 DSC_1540

Fig. 7 Query Image selected DSC_1540_tamp6

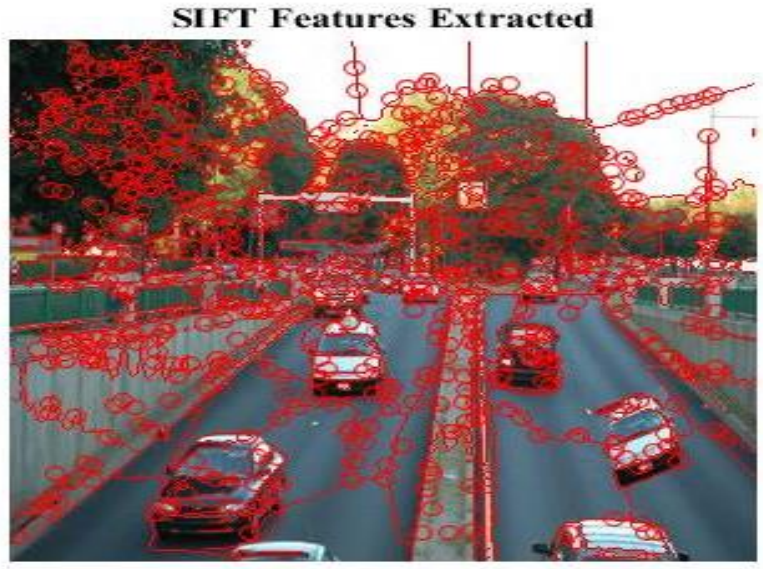

Fig. 8 SIFT feature extracted from query Image 2 Tampering-6

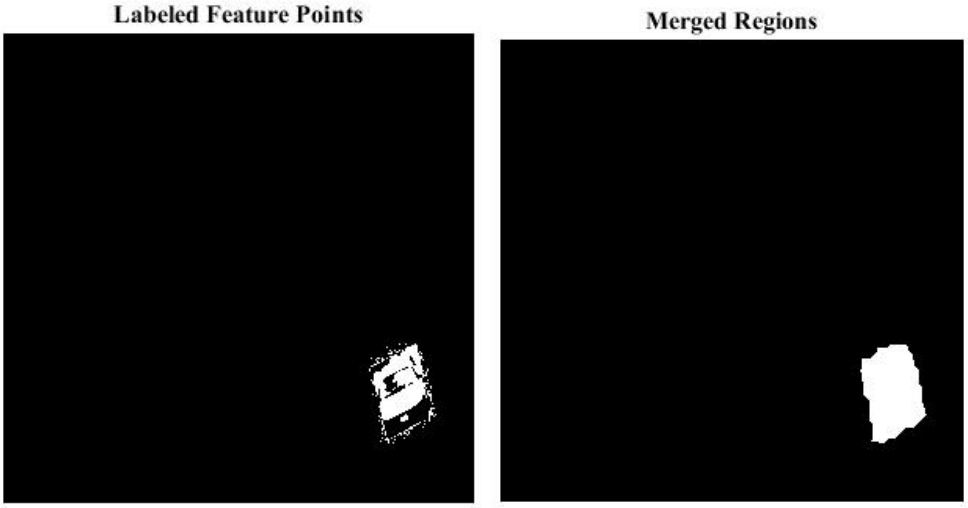

Fig.9 (a) Forged Region Labeled in Query Image 2 Tampering-6
(b) Merged Region for boundary detection for Image 2 Tampering-6

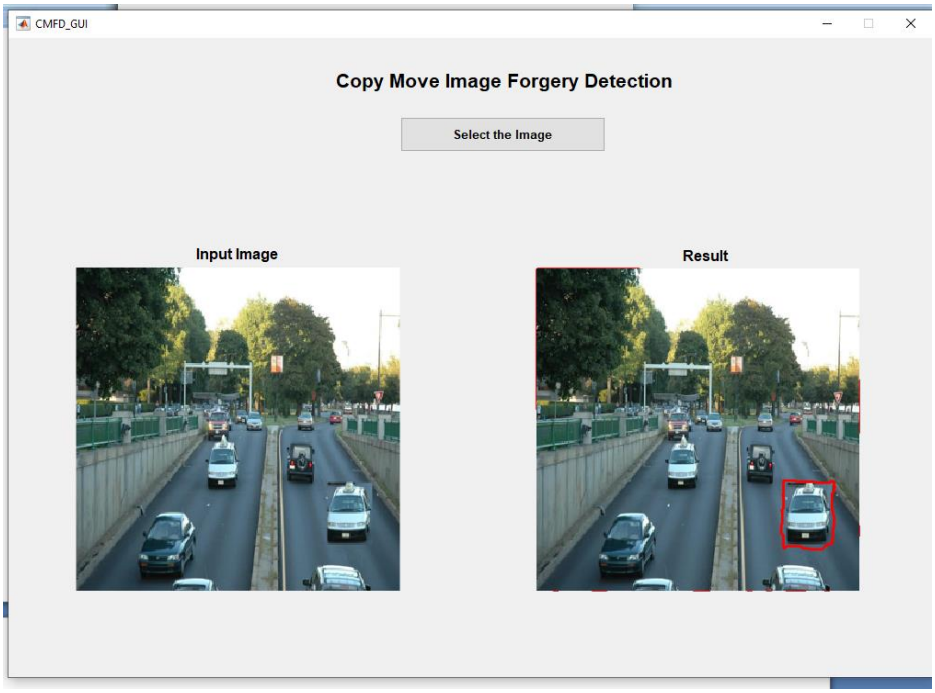

Fig. 10 Final Result with Forged region detection for Image 2 Tampering-6

4.3 Result Analysis

145 images were tested in MA TLAB using the proposed method. 60 of the images were forged and 85 were original. The algorithm was tested and verified using the database of MICC-F220 [7].

The time required for computation was 2.893 seconds. It was found that smaller the size of the test image and the copied part, lesser were the number of features found. Time required for computation of different test images was found to be different and the average time centered around 2s.

Few terms are defined:

TP (True Positive): Forged image identified as forged

FP (False Positive): Authentic image identifies as forged

TN (True Negative): Authentic image identified as authentic

FN (False Negative): Forged image identified as authentic

Performance of any system can be measured in terms of sensitivity, specificity and accuracy. Sensitivity relates to theability of the algorithm to detect a forged image correctly as forged. Specificity relates to the ability of the algorithm to identify an authentic image correctly as authentic. Hence a high value of sensitivity and specificity imply better performance of the system.

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

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

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

$$FPR = 1 - Specificity\ (False\ Positive\ Rate)$$

$$FNR = 1 - Sensitivity\ (False\ Negative\ Rate)$$

Following table 1 and shows the performance of the proposed system based on various parameters.

Table 1 Result of the Proposed System

No of Authentic images	No of Forged Images	TP	TN	FP	FN
60	85	81	57	3	4

Table 2 Performance of the Proposed System

Sensitivity (%)	Specificity(%)	Accuracy(%)	FPR(%)	FNR(%)
95.29	96.00	95.17	4	4.71

4.4 Comparison with Similar Systems

The preceding sections have covered a few important algorithms and their shortcomings. The accuracy of the suggested approach and other approaches was contrasted. Zhang-2008[53] used the modified region size of 64x64 and obtained an accuracy of 77.32%. For a tampered block size of 128x128 in an image of size 512x512 and a JPEG

quality factor of 85, the Popescu-2004[54] approach achieved an accuracy of almost 90%. Li2009 [55] had a 47.21% accuracy rate. However, excellent sensitivity and specificity scores made up for this low accuracy number. Over 145 photos, the suggested method's accuracy was 95.17%. It should be mentioned that the suggested approach is solely intended for copy-paste forgery detection.

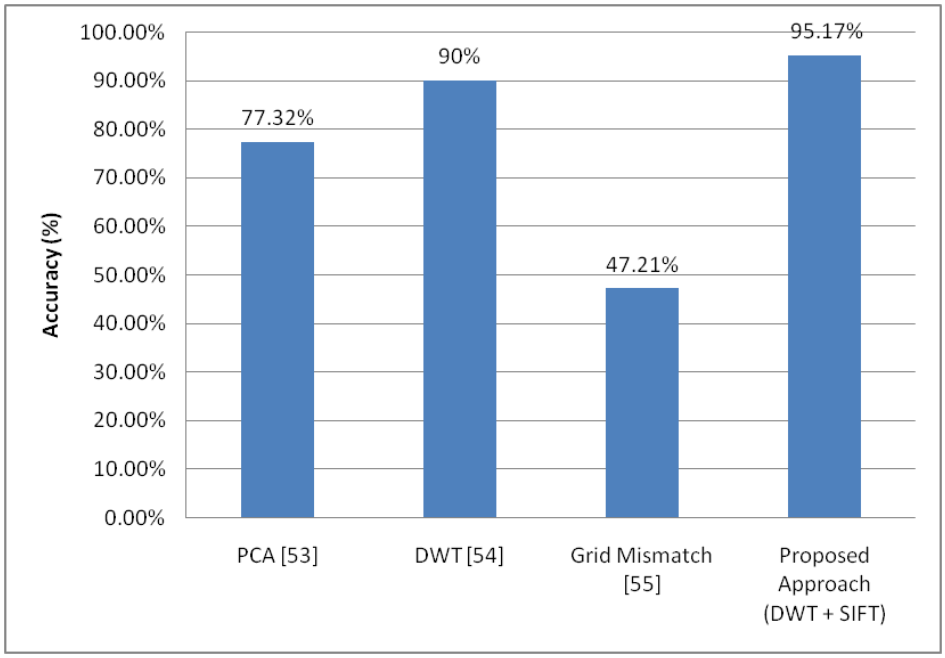

Fig. 11 Comparison with Similar System

V. CONCLUSION

This paper presented a comprehensive study on copy-move forgery detection (CMFD) in digital images. After reviewing existing state-of-the-art techniques, it was observed that while keypoint-based methods (such as SIFT and SURF) are computationally efficient, they often lack accuracy in detecting forgeries in flat regions. On the other hand, block-based methods offer better precision but are computationally intensive.

To address these limitations, a hybrid approach combining Discrete Wavelet Transform (DWT) and Scale-Invariant Feature Transform (SIFT) was proposed. DWT was employed for dimensionality reduction and feature enhancement, while SIFT provided scale and rotation invariance for robust feature matching. This integrated method significantly improved the accuracy and speed of forgery detection.

The system was tested on standard datasets (MICC-F220), and experimental results demonstrated an impressive average accuracy of 95.17%. The method was capable of identifying tampered regions effectively, even under geometric transformations like rotation and scaling. The simulation results validated the proposed approach as a reliable and efficient solution for detecting copy-move forgeries in digital images.

However, limitations were also observed—particularly in detecting multiple forged regions and forgeries in homogeneous or flat texture areas. These areas present opportunities for further refinement.

REFERENCES

[1]. Saiqa Khan, Arun Kulkarni, “Reduced Time Complexity for Detection of Copy-Move Forgery Using Discrete Wavelet Transform” International Journal of Computer Applications (0975 – 8887) Volume 6– No.7,September 2010, pp 31-36.

[2]. Sunil Kumar, Jagannath Desai, Shaktidev Mukherjee “A Fast DCT Based Method for Copy Move Forgery Detection”, In Proceedings of 2013 IEEE second International Conference on Image information processing (ICIIP-2013), pp 649-654.

[3]. Neha Jadhav, Suvarna Kharat, Punam Nangare “ Copy Move Forgery Detection Using DCT”, International Journal of Emerging Technologies and Engineering

(IJETE)Volume 2 Issue 3, March 2015, ISSN 2348 – 8050, pp 38-42.

[4]. Ashima Gupta, Nisheeth Saxena, S.K Vasistha, “Detecting Copy move Forgery using DCT”, International Journal of Scientific and Research Publications, Volume 3, Issue 5, May 2013, pp 1- 4.

[5]. Muhammad, Najah, Muhammad Hussain, Ghulam Muhammad, and George Bebis, "Copy-move forgery detection using dyadic wavelet transform.", In Proceedings of IEEE Eighth International Conference on Computer Graphics, Imaging and Visualization (CGIV2011), pp. 103-108.

[6]. Huang, Hailing, Weiqiang Guo, and Yu Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm", In Proceedings of Pacific-Asia Workshop on Computational Intelligence and Industrial Application (PACIIA-2008), vol. 2, pp. 272-276.

[7]. N.Anantharaj, “Tampering and Copy-Move Forgery Detection Using Sift Feature”, International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Special Issue 1, March 2014, pp 2132-2137.

[8]. Prabhaka Telegarapu, V. Jagan Naveen, A. Lakshmi Prasanthi, G. Vijaya Sant, “Image Compression Using DCT and Wavelet Transformations”, International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol 4, No.3, September 2011, pp 61-74.

[9]. Xiaolong Li. “General Framework to HistogramShifting-Based Reversible Data Hiding”, IEEE Transactions of image processing, Vol. 22, No. 6, June 2013, pp 2181-2191.

[10]. Li, Weihai, Yuan Yuan, and Nenghai Yu. "Passive detection of doctored JPEG image via block artifact grid extraction." Signal Processing, vol. 89, no. 9, September 2009, pp 1821-1829.

[11]. Amanpreet Kaur, Rich Sharma“ Copy-Move Forgery Detection using DCT and SIFT” International Journal of Computer Applications , Volume 70– No.7 , May 2013 , pp 30-34.

[12]. Salam A. Thajeel,.“A Survey of Copy Move Forgery Detection Techniques”, Journal of Theoretical and Applied Information Technology, Vol.70 No.1, 10th December 2014, pp 25-35.

[13]. Rohini. A. Maind, “Image Copy Move Forgery Detection using Block Representing Method”, International Journal of Soft Computing and Engineering , Volume-4, Issue-2, , May 2014, pp 49-53.

[14]. Popescu, Alin C. , and Hany Farid, "Exposing digital forgeries by detecting duplicated image regions", Department of Computer Science Dartmouth College, Technical Report, August 2004, pp 1- 11.

[15]. Nandini Singhal and Savita Gandhani, “Analysis of Copy-move Forgery Image Forensics: A Review”, International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.8, No.7 (2015), pp.265-272.

[16]. Vincent Christlein, Christian Riess, Johannes Jordan, Corinna Riess, Elli Angelopoulou “An Evaluation of Popular Copy-Move Forgery Detection Approaches”, IEEE Transactions on Information Forensics & security, Vol 7, No.6, December 2012 , pp 1841-1854.