

# Performance Evaluation of Copy-Move Forgery Detection of JPEG Compression

Vishalkumar J Vankar<sup>1</sup>, Krunal J. Panchal<sup>2</sup>

<sup>1</sup>Research Scholar, Computer Engineering Department, L.J. Institute of Engineering & Technology, Gujarat, India

<sup>2</sup>Assistant Professor, Computer Engineering Department, L.J. Institute of Engineering & Technology, Gujarat, India

## ABSTRACT

The paper present a new method to detect forgery in manipulate copy-move images. Proposed method based feature comparison. Three level Discrete Wavelet Transformation (DWT) decomposition for a multiresolution. Canny edge detector used to identify the edges in the image and binary frame used for boundaries identify. Applying X-OR operation to compare feature points. Using binary frame boundary and X-or operation identify duplicate region in copy-move images. our method also work with duplicate regions with scaling in Duplicate image and lossy JPEG compressions.

**Keywords :-** Copy-Move forgery, 3 Level DWT, binary frame, X-OR operation..

## 1. INTRODUCTION:

Now a days image forgeries are common problems as we know the image forgery can be done by using simple image editing tools such as Windows Image editor, GIMP image editor and Photoshop etc. So it is very difficult to decide the given image is original or forged one with our naked eye and as we know it is very much important to identify an unforged image to take a right decisions.

• Types of Digital image forgery:

1. Image Retouching: this is a less harmful than a other forgery methods. In this method certain features or parameters of the image are enhanced or degraded.[5]
2. Image Splicing: most common manipulation method. In this method forgery can be defined as a cut-and paste of image regions from one image onto the same or another image without post processing.[5]
3. Copy-Move: in which certain portions of the image are copy pasted in the same image to conceal a person or objecting the scene.[5]



**Fig -1:** Example of Forgery[4]

- Digital images forgery detection approaches:
  1. Active approaches: certain information is embedded inside an image during the creation or before the image is being disseminated to the public Example: Water marking[5]
  2. Passive approaches: Passive method does not require any pre-image distribution information which is to be inserted into a digital image. Example: JPEG compression, Wavelet transformation[5]

## 2. LITERATURE REVIEW:

- Edoardo Ardizzone et. al [1] proposed a method for copy-move detection based on triangles of keypoints. Instead of searching similar small blocks to detect the copied objects, this paper looks for the similar triangles which are connected by a Delaunay triangulation from interest points in image using SIFT, SUFT and Harris. Pixels in a triangle have similar features. By this method, each triangle can be described by dominant color, inner angles, descriptor vector. Triangles are matched by comparing both color and inner angles or mean vertex descriptor which is the average of descriptor vectors. Post-processing to fill the holes between triangles and increase the recall in simulation is also suggested for the future.
- Increase the efficiency of DCT in duplicated regions detection algorithm is proposed by Elham M. et. Al[2] . Copy-Move images are firstly converted to grayscale and specified into complex or smooth images based on the number of white and black pixels in binary image which are obtained from the Canny filter. Image is split into overlapping 8x8 or 16x16 blocks before applying DCT to extract features of these small blocks. Duplicated regions are detected from block matching, which are obtained by comparing feature vectors. The effectiveness of this method is to detect copy-move forgery such as image compression and Gaussian blur. If the noise is added with considering the size of blocks in smooth and complex Images will increases the accuracy of forgery detection.
- Gunjan Bhartiya, Anand Singh Jalal [3] proposed a fast and accurate algorithm for copy-move forgery detection. First image is split than a produce a feature vector, using feature vector build K-D tree. Find a near duplicates nodes in the K-D tree, then after obtain a histogram of each block. Applied block matching method detect forgery. This method compared new proposed algorithm with the state art method to test its robustness. In a feature work check the availability and reliability of converting the algorithm into a parallel one.
- Mohsen Zandi, Ahmad Mahmoudi-Aznaveh and Alireza Talebpour[4] proposed a method to Utilize the advantages of block based and Traditional key point based method. Interest point detector, Adaptive matching and filtering are the main process of this method. a novel interest point detector Specialized for CMFD is proposed certainly cover the whole image in a compact manner. So the matching process is more reliable in distinct areas. In future they plan to improve interest point detector by means of scale-space technique to order to deal with resizing attack.
- Huynh Kha Tu<sup>1,2</sup>, Le Tien Thuong<sup>1</sup>, Ha Viet Uyen Synh<sup>2</sup>, Huynh Thanh Son<sup>3</sup>, Huynh Van Khoa<sup>1</sup>[5] proposed a new method to detect the forgery in Copy-Move images using feature comparison to find the similar parts and

sharpness estimation to collect the suspicious edges. one-level DWT decomposition, with the role of multiresolution, is used to limit the computational complexity and morphological operation is applied for presenting counterfeit objects. Both feature comparison and sharpness are done in overlapping 16x16 blocks of LL and HH sub-bands. Searching similar blocks in approximation part by modified Zernike Moments and calculating the sharpness of edges in HH sub-band confirm the copy-move objects in image. Faked regions have features similar to any other image's region and sharpness at boundaries higher than at other edges in the image. The combination of LL and HH sub-band can improve the reliability of the detection. The suspicious regions are then colored by opening and closing of morphological analysis and shown by logical operator "AND" to the tested image. The fact that similar regions can be detected and defined to be copy-move or same texture is the novelty of the proposed method. Detecting duplicate regions with scaling is a feature work for this paper.

### 3. PROPOSED METHOD:

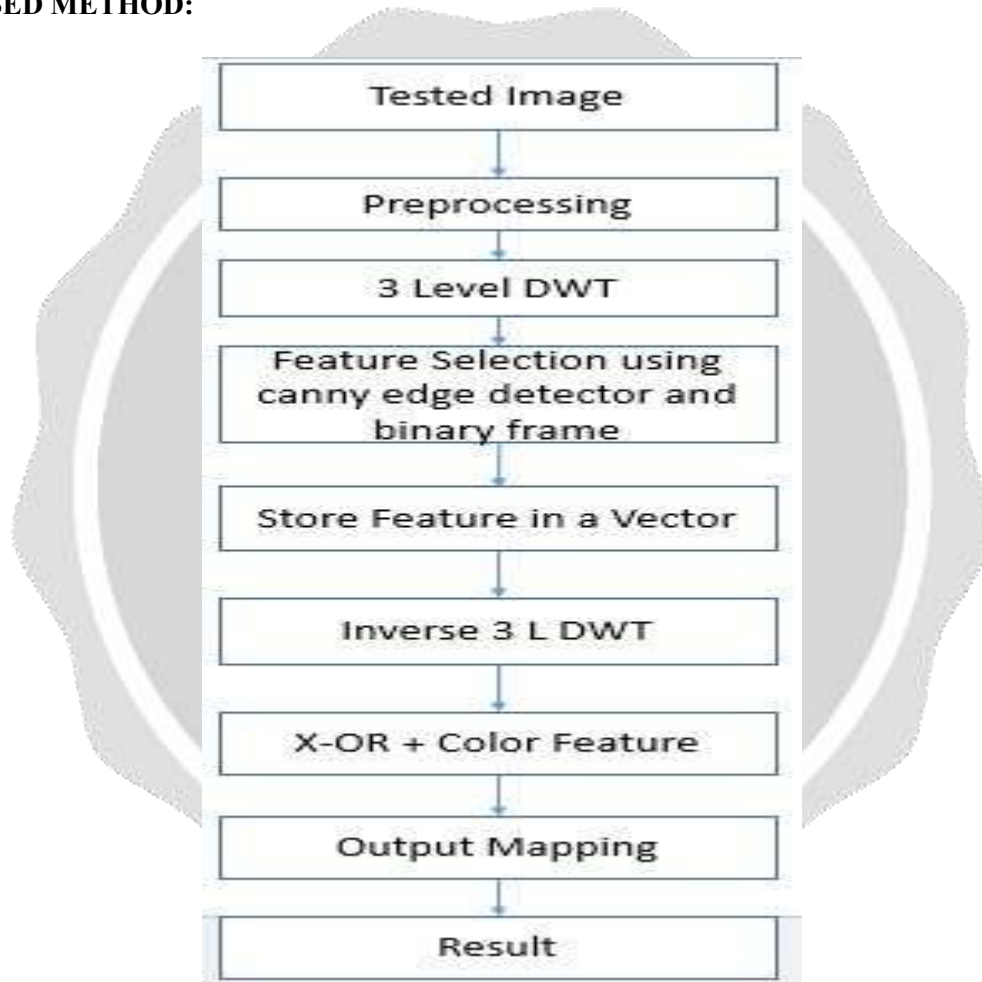


Figure 2: Proposed Flowchart

**4. RESULT ANALYSIS:**

For a result analysis we calculate precision rate and recall rate.

- Precision Rate: The precision rate is defined as the ratio of correctly detected parts to the sum of correctly detected parts plus false positive.

$$\text{Precision Rate (p)} = \frac{\text{Correctly detected parts (T}_p\text{)}}{\text{Correctly detected parts (T}_p\text{)+ False Positives(F}_p\text{)}}$$

- Recall Rate: The Recall rate is defined as the ratio of correctly detected parts to the sum of correctly detected parts plus false negatives.

$$\text{Recall Rate (r)} = \frac{\text{Correctly detected parts (T}_p\text{)}}{\text{Correctly detected parts (T}_p\text{) + False Negatives (F}_N\text{)}}$$



Original Image

Copy-move image

Mark the duplication

Detection

Normal Copy-Move image



Original image

Copy- move image

Mark the Duplication

Detection

Copy-Move image with Rotation





Copy-Move Image with Scaling

Copy-Move forgery with different angle	Precision (p)	Recall (r)
Normal Copy-Move image Forgery	98.132%	96.47%
Copy-Move image Forgery with Rotation	96.85%	94.23%
Copy-Move Image Forgery With Scaling	97.47%	94.96%

**4. CONCLUSION:**

In this paper, DWT based method is used detect Copy-Move Forgery and also provided shape and size of manipulated area, even after processing such as image compression formats. The novelty our proposed method to detect copy-move forgery with different type shape like as rotation and Scaling. Result analysis evaluation by precision rate and recall rate. Now in feature implement forgery detection method to considering to complexity of images that distorted by Gaussian white noise.

**5. REFERENCES:**

[1] Edoardo Ardizzone; Alessandro Bruno; Giuseppe Mazzola, “Copy–Move Forgery Detection by Matching Triangles of Keypoints”, IEEE Transactions on Information Forensics and Security, Pages: 2084 - 2094, DOI: 10.1109/TIFS.2015.2445742, Volume: 10, Issue: 10, 2015.

[2]. Elham Mohebbian; Mahdi Hariri, “Increase the efficiency of DCT method for detection of copy-move forgery in complex and smooth images”, the IEEE 2nd International Conference on Knowledge-Based Engineering and Innovation (KBEI), Tehran, 2015

- [3]. Abdullah M. Moussa, "A fast and accurate algorithm for copy-move forgery detection", 2015 Tenth International Conference on Computer Engineering & Systems (ICCES), Cairo, 2015.
- [4]. Mohsen Zandi, Ahmad Mahmoudi-Aznaveh, Alireza Talebpour, "Iterative Copy-Move Forgery Detection Based on a New Interest Point Detector", IEEE Transactions on Information Forensics and Security, DOI: 10.1109/TIFS.2016.2585118, Issue 99, 2016.
- [5]. Huynh Kha Tu<sup>1,2</sup>, Le Tien Thuong<sup>1</sup>, Ha Viet Uyen Synh<sup>2</sup>, Huynh Thanh Son<sup>3</sup>, Huynh Van Khoa<sup>1</sup> " Develop an Algorithm for image Forensics using feature comparison and sharpness estimation" 2017 International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom), DOI: 10.1109/SIGTELCOM.2017.7849800,.
- [6]. Vincent Christlein," An Evaluation of Popular Copy-Move Forgery Detection Approaches", IEEE Transactions On Information Forensics And Security, 2011.
- [7]. G. Cao, Y. Zhao, R. Ni and X. Li, "Contrast Enhancement-Based Forensics in Digital Images," IEEE Trans. Inf. Forensics Security, Mar. 2014.

