International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT217333

# Image Forgery Detection and Localization

**Aditi Shedge*[1], Shaily Shah[1], Shubham Pandey[1], Mansi Pandey[1], Rupali Satpute[2]**
*[1]Student, Department of Electronics and Telecommunication Engineering, K.J. Somaiya Institute of Engineering and Information Technology, Mumbai, Maharashtra, India
[2]Assistant Professor, Department of Electronics and Telecommunication Engineering, K.J. Somaiya Institute of Engineering and Information Technology, Mumbai, Maharashtra, India

**Article Info**
Volume 7, Issue 3
Page Number: 176-182

**Publication Issue :**
May-June-2021

**Article History**
Accepted : 10 May 2021
Published : 16 May 2021

## ABSTRACT

A human brain responds at a much faster rate to images and the information it contains. An image is considered as proof of past events that have occurred, but in today's world where editing tools are made available so easily tampering of images and hiding the original content has become too mainstream. The identification of these tampered images is very important as images are considered as vital sources of information in crime investigation and in various other fields. The image forgery detection techniques check the credibility of the image. Various research has been carried out in dealing with image forgery and tampering detection techniques, this paper highlights various the type of forgery and how they can be detected using various techniques. The fusion of various algorithms so that a complete reliable type of algorithm can be developed to deal mainly with copy-move and image splicing forgery. The copy-move and image splicing method are main focus of this paper.

**Keywords :** Image Forensics, Image Integrity Detection, Forgery Detection, Forgery Localization, Copy Move Detection, Discrete Cosine Transform

## I. INTRODUCTION

WHY IMAGES ARE SO IMPORTANT? As it is rightly said that a good image is worth 10,000 words. In today's digital world especially the importance of image is very much relevant in the current ongoing pandemic where the source of information are images. Manipulating and tampering the digital images and creating a completely fake image without leaving any traces behind becomes very easy with the availability of easy and powerful photo editing tools. This results in rapid increase of manipulation and tampering of images over the internet and the mainstream media at an alarming rate. The availability of various software's both in smartphones and computers allow almost everyone to modify the image and publish them publicly. Image forensics mainly deals with image tampering detection. With the increasing use of sophisticated easy to use photo editing software's it has become difficult to identify whether the image considered is tampered or not. Tampering of images for personal benefit leads to decrease in credibility of image. Digital images are a well-received source of information and its

credibility is very important. Therefore, image forensics have gained considerable attention during the past decade. Image's forgery classification can be done using two approaches: Active approach and Passive Approach. The maintenance of integrity and authenticity of digital images is a major problem. Generally, there are two main problems in image forensics, one is forgery detection and the other one is forgery localization. Forgery detection mainly deals with determining if an image is edited by using editing tools and performing operations such as image splicing and copy move method whereas forgery localization deals with pointing out the area in a fake image which is being manipulated.

### 1.1 Literature Review

As various techniques are available to tamper images so there is a requirement of such techniques which can contribute in maintaining authenticity and integrity of images. On a broader level, Image forgery detection techniques can be categorized into two categories: Active and passive. Digital signatures and watermarking are active techniques of forgery detection. These techniques are high in cost as only few expensive cameras have the quality to imbibe certain features which are necessary for active methods. These methods use encryption and decryption methods for ensuring the credibility of the image. Passive forgery techniques are also called non-intrusive or blind image forgery techniques. There is no requirement of any prior information about the source image. In this paper we have studied about various techniques used within copy-move forgery detection; how feature extraction is done using these techniques; their limitations. This is followed by image splicing forgery detection technique. And in last section of this paper, we have proposed a model for copy move forgery detection.[1]

### 1.2 Copy Move Forgery Detection

Copy and move forgery is one of the most common and easy type of forgeries in which, a part of any image which can have any dimension and shape is copied and pasted over that same image at different location in image, pasting can be single or multiple, essence of that copy and paste is that it performed over same image to hide or manipulate some important feature/information of image. Here source and destination image of forgery is a single image. This tampering is mainly about copying some region from image it has different approach to tamper any image, some use that region directly, some apply some transform like scaling, rotation, skewing, stretching and flipping over copied portion so they fool the detector and make a similar copy near to original so it makes detection difficult. There are several techniques to detect the number of forgeries in images. This technique can be further classified into block based and key-point based technique.[3]


**Fig -1**: Copy Move Forgery

### 1.3 Image Splicing Detection

In today's world where everything is managed through social media platforms images play a very important role in maintaining the authenticity of content that is being shared. Let's take the example of newspapers and magazines that we read daily rely on images for proper representation of the

information that is happening around the globe. Hence, we can say that original analog data has been replaced by the digital data. At the beginning of digital advancement, the changes were done to enhance the image performance but later on people started to tamper the contents of the image using n-number of photoshop editing tools available. Image splicing is one of the most commonly used image forgery method hence it becomes an important area of study. Fig2:is an example of image splicing along with authentic image. In Image splicing forgery a completely new fake image is created by using simple cut and paste operations. Unlike copy-move forgery there is no requirement of any post-processing method like image filtering, color enhancement, smoothening of the boundaries etc. Since splicing can be done with such ease it is a desirable topic of study in image forensics.

## II. METHODS AND MATERIAL

### 1. BLOCK BASED TECHNIQUE

In the block-based method, the image on which forgery has to be detected is divided into either overlapping or non-overlapping blocks these blocks are uniform in size. After this feature extraction is done using techniques like PCA, DCT, DWT, SVD which is applied on each individual block. The major advantage of this technique is the detection of forgery, it is highly robust against certain features like compression, scaling etc. In this paper, some of the techniques used under block-based copy move forgery detection is studied. We have used discrete cosine transform technique in the proposed model and the result.[4]

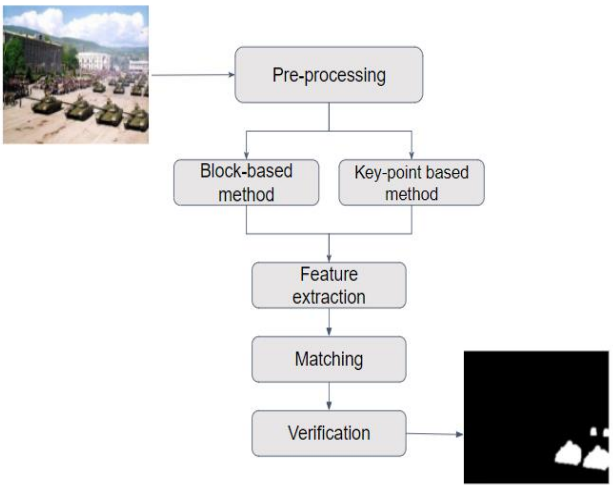


**Fig -2**: Flow diagram of CMFD

### 1.1 Singular Value Decomposition

The Singular Value Decomposition (SVD) is an algebraic modification applied to the image for detection of forged areas This technique has low computational complexity also in areas within the image where there is low noise in duplicated regions this technique is found to be highly effective. This process was not found to be effective in areas where two matched blocks were pasted and it also had no effects in jpeg compression. In SVD the given image is basically divided into three matrices, each of these matrices have built-in features which are found to be very helpful in extraction of feature. This method is also used as a post-processing step, where significant feature can be applied to the image before final display of the image.

### 1.2 Principle Component Analysis

Principle Component Analysis (PCA). This method is based on the extraction of features from an image block. In this method, the image is transformed into gray-scale and divided into many parts, which are represented by vectors. These blocks are arranged in lexicographic order with reference to the pixel intensities. After arranging, each block is accumulated in one row of a matrix. It is capable of detecting even minor variations because of noise or

lossy compression. This proposed technique is basically used for gray-scale images and also includes every color channel in color images and PCA is used to check its genuineness. The advantage of this method is that it can locate multiple duplicated regions and have the minimum number of false positives but its robustness is very weak. Also, the computational complexity and time taken to detect the forged part is comparatively high.[3]

### 1.3 Discrete Cosine Transform

In order to calculate DCT coefficients, DCT is applied to each block. Matching pairs are found by calculating and normalizing the shift vectors. Now for detecting the tampered regions in the forged image, all pairs of blocks are found which have normalized shift vectors greater than the threshold value. The quantized blocks are then subdivided into non-overlapping blocks of uniform size. For detecting duplicated regions, the mean of DCT coefficients of each of this sub-block is calculated. This technique has been used and results are found to be providing a good accuracy rate in detection of the forged part and its localization.

## 2. KEY POINT BASED TECHNIQUE

The key points of images are basically interest points within the image that means these key points do not change or get disturbed even if the image is modified, rotated or any other kind of digital techniques are used to change the contents of the image. The key point-based algorithms in the literature usually require two steps for detecting and describing general visual features i.e., identification and selection of regions within the image that has high entropy value. In the first step, the localization of the interest point is done. In the second step, the construction of the robust local descriptors is done, such that it should be invariant to affine transformations. The local visual features have been widely used for image retrieval and object recognition, due to its robustness to several geometrical transformations such as rotation, scaling, occlusions and clutter. In the literature, key point-based copy-move forgery detection is mostly based on SIFT and SURF both. A Survey on Key point Based Copy-Paste Forgery Detection Techniques of them are image local feature description algorithms based on scale-space. In this paper, we review the methods based on these techniques.

### 2.1 Scale Invariant Feature Transform (SIFT)

The SIFT based key-point technique uses computer vision to identify and extract features from the given image. Scale Invariant Feature Transform was developed by David Lowe in 2004 as a continuation of his previous work on invariant feature detection (Lowe, 1999). The author proposed a method for detecting distinctive invariant features from images that can be later used to perform reliable matching between different views of an object or scene. The main key concepts used here are: first is the distinctive and clear invariant features and second is reliable matching. The features detected by SIFT are more suited for reliable matching in the images, as it uses the cascade filtering approach to detect the features that transform image data into scale-invariant coordinates relative to local features. It consists of four main steps 1) Scale-Space extrema detection; 2) Key point localization and filtering;3) descriptors. The Speed Up Robust Feature detector (SURF) ensures the high speed in three of the feature detections steps: detection, description, and matching. Due to the use of the Hessian matrix's trace, the matching speed has been significantly improved over the SIFT. The SURF algorithm speeds up the SIFT's detection process without scarifying the quality of the detected points. Here the scale-space is created by selecting the different size box filter convolved with the integral image. The potential key points are detected by using the Hessian matrix and Non-maximum suppression.

## 3. IMAGE SPLICING DETECTION

Image splicing forgery a completely new fake image is created by using simple cut and paste operations. Unlike copy-move forgery there is no requirement of any post-processing method like image filtering, color enhancement, smoothening of the boundaries etc. Since splicing can be done with such ease it is a desirable topic of study in image forensics. There are three broad area of image tampering that is enhancement of image, morphing of image and image composting. Image splicing is a part of image composting. Using this method, the given image is divided into multiple overlapping blocks, then to adjust the select illuminant estimation algorithm a classifier is being used which is based on block content. Illuminant colour is determined on each block, and the dissimilarity between them is calculated. In case the dissimilarity is larger than a threshold, the equivalent block is categorized as a spliced block.[4]

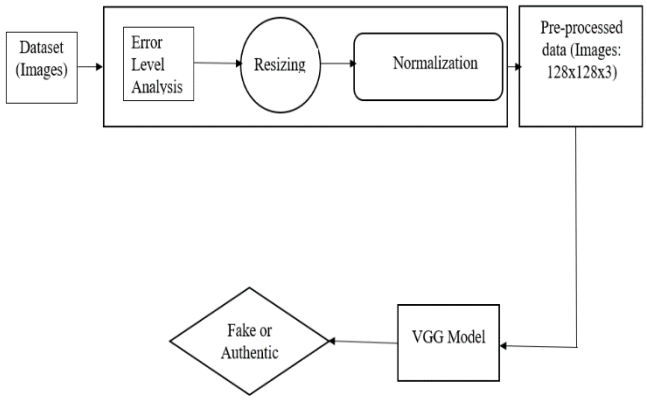


**Fig -3**: Flow diagram of Image Splicing Technique

### 3.1 Block DCT coefficients

The DCT blocks contain useful information that can be used for detecting image splicing. A new selective feature representation has been put forward based on the analysis. On the basis of practical results that has been obtained, it is noted that the new feature representation provides better results as compared to that of the traditional approach method used before. Further study showed that using Markova algorithm the blocks can be divided into inter and intra blocks which has improved results.

### 3.2 Using correlation among pixels

The method is based on stability check of color dispensation in the vicinity of edge pixels. Hue histogram entropy is then figured out to capture deformity of color distribution at these partitions. In case there is instability found in the color dispensation then this can be used to detect the area where the image is being spliced.

### 3.3 Run length-based method

For the given image gradient is calculated after which run-length is calculated. The features are constructed from the histogram of the approximate run-length. This is applied on error images and the reconstructed images for better accuracy and then the SVM is used to differentiate between the spliced and authentic image.


**Fig -4**: Image Splicing Technique

### 3.4 Error Level Analysis

Error Level Analysis is one of the techniques used for detecting image manipulation by way of storing pictures on the anniversary of a certain quality level and calculating the comparison between its levels. In General, this technique is performed on an image that has a lossy format (lossy compression). Picture type used in mining this data is JPEG. On JPEG images, compression is done independently for each 8 x 8 pixels in the image. If an image is not manipulated, each 8 x 8 pixel on the image must have

had the same error level. With JPEG, saving a picture causes the colors to change a little. The ELA results highlight the areas in the image that are most prone to color degradation during a resave.[3]

## III. PROPOSED MODEL

We have designed our model in such a way that it can be useful for detection of copy-move forgery. In the first step image is converted into grayscale image as a part of pre-processing step and then some initialization of vector takes place. We have used discrete cosine transform for extraction of features and removal of unwanted noise from the image. Once the DCT is applied and feature is extracted, matching of vector takes place in case of any dissimilarity is found that vector is declared as vector with some digital modification done on it for that a forged image where the two tanks on the right are tampered is taken in the resultant of those two tanks are displayed with white color in the prediction mask rest of the original image is black as there is no tampering done. A better understanding of the model is depicted through the block diagram which contains the input image given to the system as well as the output obtained from the algorithm.

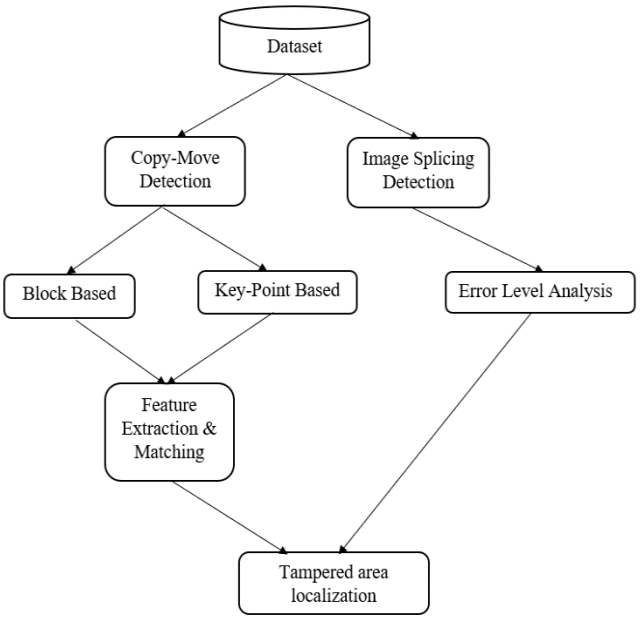


**Fig -5**: Flow diagram of Proposed system

## IV. CONCLUSION

The purpose of this paper is to analyse passive forgery techniques, focusing mainly on the most common and easy forgery method i.e., copy-move and image splicing. Copy-move forgery and image splicing forgery in the digital world is taking place at a very high rate. The rapid growth of the image processing techniques, forgery detection has become an important demand and need of the society. It is mainly being used for illegal purposes. So, to minimize these illegal acts, many techniques have been developed to handle different types of forgeries. In this paper, we have discussed mainly the copy-move forgery detection techniques and have observed that still there are many challenges related to the robustness and computational complexity in the field of forgery detection. For making a robust system against the geometric transformation attack local features of the image may be considered which are invariant against the rotation and scaling. Also, one particular technique alone cannot fulfill all the requirements for an efficient system at a time. Passive move forgery comprises various techniques out of which only two of them are studied. Simultaneously the image splicing techniques have been studied as a lot of research has been done and many methods have been proposed based on various image dimensions some of them are analysed in this paper. To resolve this issue, one or more techniques should be combined to get the desired results. In the proposed model we found that DCT works at much faster rate with less computational complexity involved. Although DCT has some limitations when it comes to localization of forgery within the image, the detection rate of DCT is quite good as compared to other block-based copy-move forgery detection techniques.

## V. REFERENCES

[1]. Tao Chen, Jingchun Wang and Yonglei Zhou1"Combined Digital Signature and Digital Watermark Scheme for Image Authentication" of Department of Automation, Tsinghua University, Beijing, 100084, P.R. China 2 State Key Lab on Pattern Recognition, Beijing, 100080, P.R. China

[2]. Abhishek Kashyap, Rajesh Singh Parmar, B. Suresh, Megha Agarwal, Hariom Gupta "Detection of Digital Image Forgery using Wavelet Decomposition and Outline Analysis" Department of Electronics and Communication Engineering, Jaypee Institute of Information Technology, Noida-201304, Uttar Pradesh, India

[3]. Badal Soni Debalina Biswas "Image Forensic using Block-based Copy-move Forgery Detection" of National Institute of Technology Silchar Conference Paper February 2018

[4]. Anuja Dixit and R.K. Gupta "Copy-Move Image Forgery Detection a Review" Department of Computer Science & Engineering and Information Technology Madhav Institute of Technology & Science, Gwalior, Madhya Pradesh, 474005, India

**Cite this article as :**

Aditi Shedge, Shaily Shah, Shubham Pandey, Mansi Pandey, Rupali Satpute, "Image Forgery Detection and Localization", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 3, pp. 176-182, May-June 2021.
Available at
doi : https://doi.org/10.32628/CSEIT217333
Journal URL : https://ijsrcseit.com/CSEIT217333