Image Forgery Classification : Tampering Detection

Team - EE20BTECH11007, EE20BTECH11013,
EE20BTECH11016, EE20BTECH11059

EE6310 PPR - Team ID 17

Abstract

Images represent an effective and natural communication medium for humans due to their immediacy and the ease with which image content can be understood. The widespread availability of image editing software tools makes it easier to alter image content or create new images. As a result, the possibility of tampering and counterfeiting visual content is no longer restricted to experts. This situation underscores the need for methods to verify the truthfulness of images and assess their quality. Answering these queries is relatively easy when the original image is known. However, in practical cases, almost no information can be assumed to be known a priori about the original image, making our task difficult. This paper explores all possible methods that can be applied to detect tampering forgery and its subtypes, such as Copy-move, splicing, and part-removal.

Index Terms – Image Forgery, Tampering detection, Image Forgery Detection, Active and Passive Techniques for forgery detection.

0. Problem Statement

Our objective is to address the challenge of detecting tampering in digital images. Specifically, we aim to focus on detecting Copy-move and splicing.

1. Introduction

Image forgery has become a significant problem nowadays. With the rise of technology, many methods have been developed that can tamper with images without any visual difference. People of all classes are now exposed to such tools, allowing them to tamper with images and create Deepfakes. However, along with the increase in technology, not only has this exploitation increased, but many advanced methods for image forgery detection have also been developed, with many others currently in development. This research area, along with the wide scientific community, provides reliable methods for detecting forgery. This paper will explain briefly some of the methods we have come across and also classify image forgeries and image forgery detection techniques.

2. Image Forgery Classification

Image forgery classification is the process of identifying whether an image has been manipulated or altered in any way. With the increasing availability of powerful image editing tools, image forgery has become a significant concern in various domains such as forensics, journalism, and media content.

In order to effectively detect image forgery, it is necessary to have a comprehensive understanding of the various types of image forgery.

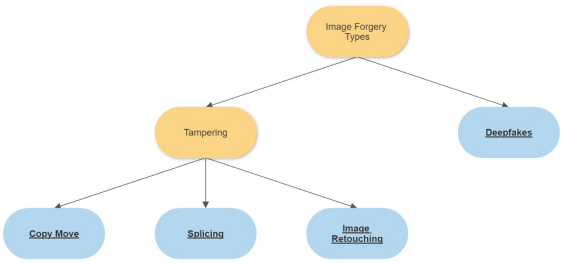


Figure 1. Classification of Image forgeries

- **Tampering** : Image tampering is the act of intentionally altering or manipulating an image in any way, with the purpose of deceiving the viewer or changing the image's original meaning or intent. The alteration can range from subtle changes, such as adjusting the brightness or color of an image, to more complex modifications, such as adding, removing or replacing objects, or merging two or more images into one. It is further divided into the following sub types:
  - **Splicing** : Image splicing can be defined as the act of cutting and pasting a portion of one im-

age into another image to create a new image that misrepresents the original context or intent.

  - **Retouching** : Image retouching can be defined as the act of enhancing, adjusting or modifying an image by removing unwanted elements, improving color, contrast, sharpness or other visual characteristics, without changing the image's original context or meaning.
  - **Copy-move** : Copy-move forgery can be defined as the act of duplicating one or more regions of an image and pasting them in another location within the same image to create a new image that misrepresents the original context or intent. Copy-move forgery is commonly used in digital image tampering to conceal or add objects in an image.

- **Deepfakes** : Deepfake refers to a technique that uses artificial intelligence (AI) algorithms, such as deep neural networks, to generate fake media, such as images, videos, or audio recordings, that appear to be real and genuine.

Let us now discuss the various forgery detection techniques and also throwing light on those approaches in brief.

3. Image Forgery Detection Techniques

The image forgery detection techniques are classified into two types mainly: Active and passive approaches. Here are images showing the classification of image forgery detection techniques from the research papers [3] and [5]

3.1. Active Techniques

Active-based image forgery detection techniques exploit some information that has been computed at the source side (i.e., in the camera), during the acquisition step.

3.2. Passive Techniques

Passive-based image forensics aims to develop algorithms for tampered image detection without using any information beyond the image itself.

The above is the general overview of all image forgeries and their detection techniques. As this research area is broad we have decided to focus on one specific forgery i.e, Image tampering and its detection (in specific we are focusing on passive techniques based detection algorithms for tampering).

4. Methods based on reviewed literature

The passive detection involves more forensics as they don't have any watermark embedding and we have to look for individual pixels of image to get some inference about the classification. For passive detection we have both traditional methods and deep learning methods to solve our problem. These are few methods for image forgery detection we have come across in the literature read:

- **Edge analysis**: Some image manipulation techniques involve copying and pasting parts of an image. By analyzing the edges of different objects in the image, it may be possible to detect whether they are inconsistent with the rest of the image. For edge detection we can use the LOG filters and also there are DL based edge detectors.

- **Noise analysis**: When an image is edited, it can create new patterns of noise that are different from the noise in the original image. By analyzing the noise patterns, it may be possible to detect whether an image has been manipulated.

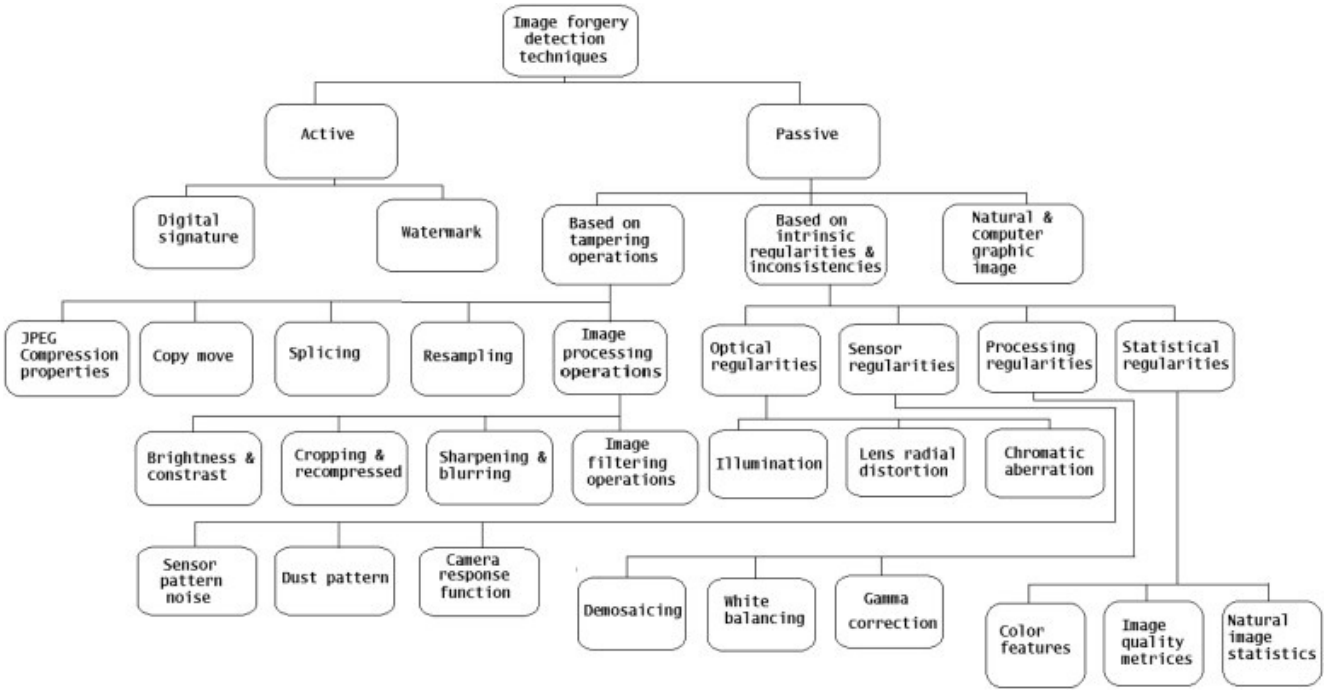
- **Error level analysis**: When an image is compressed and then re-saved, there is often a loss of quality that can create distinctive compression artifacts. Error level analysis involves detecting these artifacts by analyzing the differences in compression quality between different parts of the same image.

- **Using DCT,DWT along with SVD**: In the past people used transform techniques such as DCT(Discrete Cosine Transform) and DWT (Discrete Wavelet Transform) along with SVD (Singular Value Decomposition) to detect tampered images as used in [6], [2].

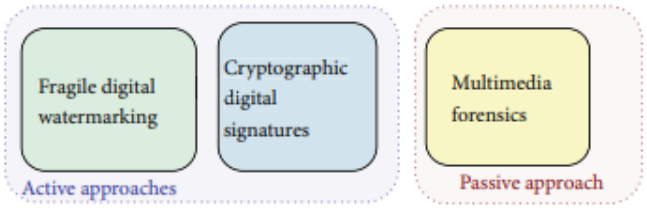
- **ML based steps for detection**: This method discussed in [1] has following steps:

  - Image Pre-processing: The first step to detect the image forgery is image preprocessing. This is performed using the process such as RGB to grey scale transformation, image enrichment, image filtering etc.
  - Feature Extraction: The picture set is separated from other classes by the features specified for each class, but the picture set remains consistent for the class chosen. The appealing aspect of the selected collection of attributes is the minute measurement, which reduces the computational complexity while providing a wide distinction from other classes.
  - Selection of Classifier: The appropriate classifier is either picked or composed based on the feature set acquired during feature extraction. Due to the huge number of training sets, the classifier performance will be enhanced.

EE6310
#17



(a) *Classification according to paper [3]*



(b) *Classification according to paper [5]*

Figure 2. Classifications of Image Forgeries Detection Techniques.

- Classification: The goal of the classification process is to only determine whether the picture is real or not. To find the originality of the image LDA, Neural systems, and SVM classifiers are utilized.
- Post-processing: A few image falsifications may necessitate post-processing that includes alterations such as confinement copy locale localization.

The above are general methods that can be applied to detect tampering and its sub types. Now we will move on to specific methods to solve splicing, Copy-move forgeries.

4.1. Copy-move Specific Detection Techniques

The key characteristics of Copy-move forgery is both the original image and the copied part are in same image so we can use this relation for accurate detection of forgery by looking for identical or duplicate image regions.
The below is the image showing common framework to detect the Copy-move forgery.

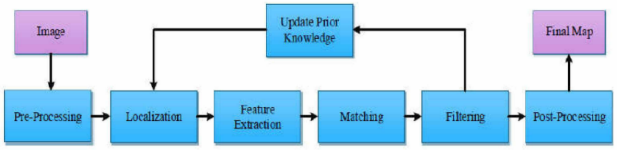


Figure 3. Common Framework Of The Copy-move Forgery Detection Technique [8]

We are considering using ML models and Neural Networks (CNN and RNN) to create a classifier that can identify tampered images and potentially determine the specific area of the image that has been affected.

4.2. Splicing Specific Detection Techniques

The key to detect a spliced image is the feature extraction which can distinguish spliced images from authentic images. Similar to Copy-move here also there are passive techniques to detect Splicing, like using DCT coefficient analysis.

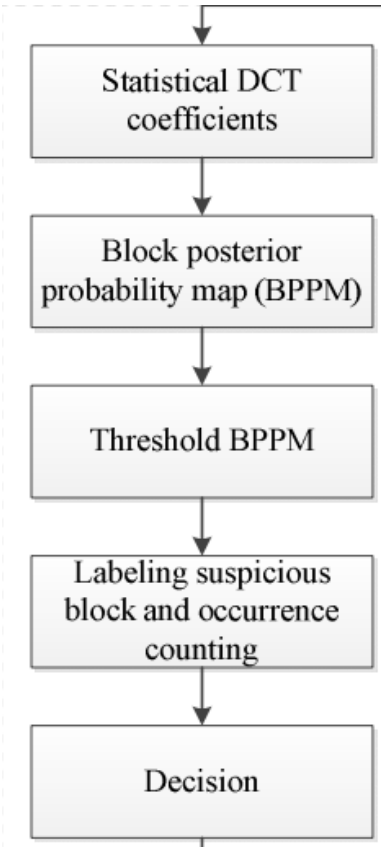


Figure 4. Flow chart of the above method [7]

We used this report [4] as our general guide for the classification of image forgery, image forgery detection techniques and will be following this to get datasets and will be building upon this.

References

[1] Pydipalli Sai Achyuth and Vella Satyanarayana. Image forgery detection techniques: A brief review. pages 234–778, 2005. 2

[2] Hasan Şakir Ahmet. Copy-move image forgery detection based on lbp and dct. 2

[3] Vijay H. Mankar Gajanan K. Birajdar. Digital image forgery detection using passive techniques: A survey. 2, 3

[4] Chao Zhang Jingjing Chen Yu-Gang Jiang Larry S. Davis Junke Wang, Zhenxin Li. Fighting malicious media data: A survey on tampering detection and deepfake detection. 4

[5] Alessandro Piva. An overview on image forensics. 2, 3

[6] Arun Kulkarni Saiqa Khan. Robust method for detection of copy-move forgery in digital images. 2

[7] Tszan Wu Shinfeng D. Lin. An integrated technique for splicing and copy-move forgery image detection. 4

[8] A. Mahmoudi-Aznaveh Zandi, M. Iterative copy move forgery detection based on a new interest point detector. 3