iJournals: International Journal of Software & Hardware Research in Engineering (IJSHRE)
ISSN-2347-4890
Volume 9 Issue 5 May 2021

A Review Paper on Digital Image Forgery Detection Techniques using Matlab Tool

Authors: Priyanka Kundal[1]; Er. Sorab Kumar[2]

Department of computer science & Engineering, Sri Sai College of Engineering & Technology Badhani, Punjab India[1,2]

Abstract

Images have the capability to render a large amount of information. With the widespread popularity of social networking services such as WhatsApp, Facebook, Instagram, Snapchat, Twitter etc., there has been a huge increase in the volume of image data that is shared instantly. This has also increased the cases of fake or forged images being shared which can have serious after-effects. Image forgery can affect the image of persons, organizations and communities and in some cases cause social unrest and violence. Due to the size and complexity of the data being shared, it is almost infeasible for manual detection of image forgery. Therefore, it has become mandatory to design automated systems which can detect image forgery in very less time and with high accuracy. Since the data size to be analyzed by time critical applications is enormous indeed, therefore the conventional techniques prove to be infeasible to detect image forgery with high level of accuracy which makes it mandatory for using automated tools. In this proposed work specific approach will be used prior to classification of the image as forged or unforged. For this task Matlab Tool will be used due to the availability of in-built mathematical tools for engineering problems.

Keywords: Image Forgery, RGB-Gray scale conversion, binarization, Feature Selection, Baye's Classifier, Classification.

1.1 Introduction

With the advent of widespread use and applications of social media, images have become the most common data format which is shared among various users instantly. The images have become extremely useful and effective due to the large amount of information that that convey and contain. Images are also the fundamental components of videos which are also called frames, while with frames per second generating videos. This is the primary reason for the widespread sharing of images on social media platforms and elsewhere. Images are a function of two spatial variables x and y mathematically given by:

$$I = f(x, y) \quad \textbf{(1.1)}$$

Here,

I represents the digital image

f represents a function of

x and y are the spatial coordinates

Images are made up of picture elements or pixels which render three critical pieces of information which are:

a) Intensity or Grayscale value
b) Spatial coordinates
c) RGB value

Since the images are shared extensively among users and are one of the most common data formats used, hence they are the ones which come under the purview of attackers who try to morph or manipulate the image so as to render a different information compared to the one that is actually intended. This gives rise to image forgery or image morphing which can play havoc on individuals, or groups or organizations. This may as well lead to social unrest in several situations where the image data can go viral and without the authenticity being checked can be again re-distributed or shared among a lot of other people thereby starting a chain reaction which is often difficult to control. Thus it is necessary to understand the basics of images, their salient features and the changes which images undergo while they are manipulated.

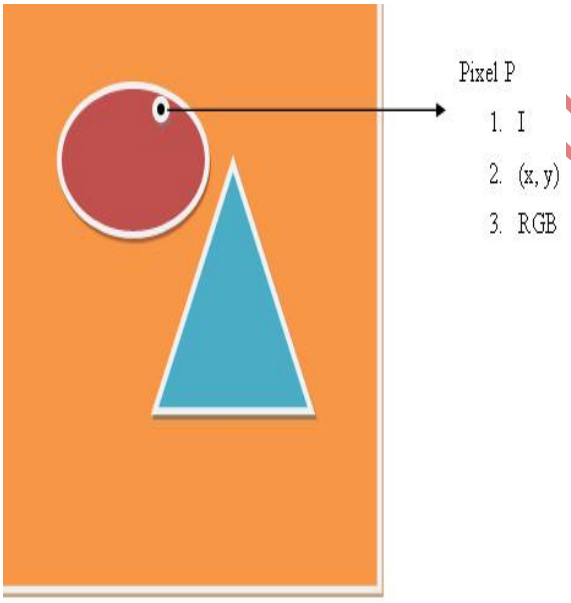

Fig.1.1 Pixel Level Representation of images

The figure above represents the pixel wise representation of an image I where the pixel P renders information about the intensity, coordinates and the RGB value. The pixels are often seen as matrices comprising of rows and columns of values. These value may have a visual perception for humans but are no more than streams of numerical values for a computing machine. The different parameters of the image may vary in accordance with the variations in the image. Now it may be challenging to access whether the variations occur due to natural causes or due to sabotaged manipulations. The natural causes can be:

1) Degradations while capturing
2) Degradations while storage
3) Degradations while transmission
4) Degradations while reception
5) Degradations while re-creation from bits

Another significant attribute is the fact that it may be challenging to predict whether the image is actually morphed or not by a computing machine since the variations arising out of the natural processes may also be competent enough to match the one arising out of deliberate effects.

1.2 Types of Digital Image Forgery

The determination of forged or unforged images needs the fundamental attributes of image forgery techniques. This can be basically categorized as image forgery with active approaches or image forgery with passive approaches. The distinction among the above is given by:

Active Approach: - This approach generally has the following attributes:

1) Pre-Processing
2) Visible changes in the texture of the image
3) A-priori information of image parameters
4) Generally performed during image creation, such as watermarking applications.

Passive Approach: - This technique has the following attributes:

1) No visible evidences of morphing
2) No apriori information needed
3) Generally a blind approach

The most common forms of passive approaches are:

Copy-Move Forgery: This technique is often referred to as cloning. In this type of manipulation, the image under consideration is analysed, then some part of the image is selected and then that part is used to shroud some other distinct part. By nature of the attack, its is challenging to make the forgery conspicuous since the properties of the same image is used to shroud some other part of the image.

Image splicing: This is one of the most common types of image forgery where one part of an image under consideration is shrouded by a part of some other image. It is more detectable compared to the copy and move approach but with the advent of new image editing tools, detection is challenging under different conditions of lighting etc.

Retouching: Retouching can be a subtle change in the image with enhancement, variation in colour or illumination of the image.

The basic categorization of image forgery techniques is given below:

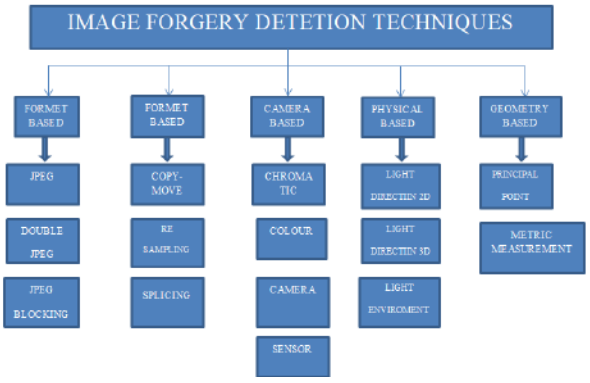

Fig 1.2 Image Forgery Classifications

1.3 Challenges In Detection Of Image Forgery

The major challenge in the detection of image forgery is the largeness of the datasets and the complexity of the images which are under consideration. A typical example of a forged and an unforged image is shown in the figure below.

Fig.1.3 Example of Forgery

The figure above illustrates the fact that the images which are under consideration are generally edited using sophisticated tools which makes it extremely difficult to recognize the forgeries with naked eyes. Moreover, for real time applications, automated systems need to be designed which can work in the bound time limits to meet the requirements of real time critical applications. This being said, the major hindrances in the detection of image forgery are the addition features listed below:

Scene complexity: Often the scene in the background is chosen such that it becomes identical to the actual image under consideration. This may include images of scenes of natural or artificial backgrounds.

Uneven lighting: The lighting is another factor which is responsible for the accurate classification of the images in categories. This being said, the ruling

factor is the number of pixels captured while capturing the image. If this is less than the prescribed or minimum number of pixels needed, a type of noise called Poisson Noise occurs which leads to blurring effects in the image.

Blurring and degradation: Blurring effects generally are caused due to:

1) Defocussing effects
2) Dearth of pixels or their orientation while image creation

Aspect ratios: The aspect ratios also play a critical role in deciding the classification of a data sample into forged or unforged category. Typically, the aspect ratio is the dimensions of pixels in the x and y spatial dimensions. Differences in aspect ratio may lead to misleading classifications of the data sets.

Similar Background: Similar background mat lead to the confusion for the classifier to classify the image into the correct category. This is due to the similarity in the pixel values that are overlapping in the case of the images which are unforged and the ones which are forged.

Non-correlation of Pixels with Classification: Pixel based classification is practically infeasible since pixels of forged and unforged images show almost no correlation. Hence simple pixel based classification is not feasible.

2.1 Literature Review

This section presents the previous work done in the domain. It highlights the salient features of the approach as well as mentions the limitation found in the approach.

Araz Rajab Abrahimet al. in [1] presented a mechanism for forgery detection in images. The features or parameters which were utilized were the histogram oriented gradient (HOG) and the local binary pattern (LBP) features. The basic edge based features and the texture based colour features were used for recognizing the image patterns. The classification was done using a feed forward neural network. The main limitation of the proposed work is the absence of comprehensive statistical features along with the texture based features. This happens to be so since the statistical features often help to detect image forgeries which are generally not distinct by analysing just the colour and texture based features. Moreover, the feed forward neural network may render low time complexity but its limitation is often in terms of the efficacy of training due to no feedback mechanism for errors.

Thales Pomari et al. in [2] proposed an approach for image forgery using Illumination Inconsistencies and Deep Learning. This approach primarily trains a deep neural network based on the features which signify inconsistency in illumination or indirectly the grayscale value of the image. The sudden changes in the illumination of the image can often render insight into the image that is then fed to the designed deep neural network which is generally a convolution neural network. The evident limitation of the proposed approach is the heavy reliance in the inconsistency in the illumination and grayscale value of images. This predominantly trains the neural network based in the intensity value of the pixels of the two categories of the images which are forged and unforged. The lack of inputs from different perspectives such as texture or statistical and probabilistic parameters often turn out to be a one dimensional approach for the classification problem limiting the accuracy of the image.

Jason Bunk et al. in [3] proposed a technique that used Resampling Features and Random Walker segmentation to train a deep neural network. The approach tries to segment out the parts of the image which seem to be morphed based on the Random Walker segmentation approach. This part is followed by the computation of resampling features. The segmentation and resampling feature computation from the segmented parts are fed to the deep neural network to classify the image. The major limitation of the approach is the necessity of segmentation of the image parts with apparent or visible modifications. While this can lead to satisfactory results for active forgery approaches, the passive approaches may clearly bypass such a segmentation based approach or render false positive or false negative values. Additionally, segmentation may result in fringing of the edges of segmenting parts which can result in plummeting values of accuracy of classification.

Clemens Seibold et al. in [4] proposed a technique for detecting facial morphing using the deep learning approach of convolutional neural networks (CNN). This approach uses the concept of one shot learning for the convolutional neural networks. The major limitations of the proposed work are the absence of distinctive pre-processing techniques which can remove the chances of noise and disturbance effects. Moreover, once shot learning doesn't rely on the separate computation of features and simply relies on the CNN based features. This happens since this neural network approach doesn't use the orientation of the image based features and the neurons do not have the capability to handle this type of feature analysis. This approach also tries to carry out a search for a specific or particular type of feature extraction and based on it, the classification is done. This means that if the features compatible with the CNN are not present, the image classification suffers heavily which is clearly undesirable.

Yuan Rao et al. in [5] proposed a technique utilizing the convolutional neural network for the detection of splicing image forgery and copy-move image forgery. The approach again uses no separate image pre-processing technique and uses the one-shot CNN learning approach. The limitations of this approach again stems from the fact that low level details regarding to the image are sent for analysis to high level neurons which again pass it forward to the next level of neural layers with the process of thresholding the features in the previous layer before passing it on the subsequent layer. This thresholding process often reduces the accuracy of the features retained for the classification process. Moreover, the lack of encapsulated neurons that can analyse the low level orientation features reduces the classification accuracy of the system. The certain neural layers that are not receptive of the low level features or even non-receptive to the thresholded feature values affect the classification accuracy adversely.

3 Conclusion

It can be concluded from the different research based on image forgery that images are widely spread through social media applications and hence there is a chance for them being viral rapidly. The size of the data being shared makes it infeasible for conventional or manual classification of images as forged or unforged. Thus automated tools are mandatory which can filter out forged image thereby mitigate the possibilities of consequences arising out of them. The proposed approach will use the image pre-processing and feature selection prior to classification of the image as forged or unforged. As per the concern with classifier in future research Baye'sclassifier will be used which works on the

principle of Baye's theorem of conditional probability. Such a probabilistic approach is effective since image pixels do not exhibit correlation with being forged or unforged. . For this task Matlab Tool will be used due to the availability of in-built mathematical tools for engineering problems.

4. References

[1] Araz Rajab Abrahim, MohdShafryMohd Rahim, Ghazali Bin Sulong "Splicing image forgery identification based on artificial neural networkapproach and texture features", IEEE 2018

[2] Thales Pomari et al. et al., "Image Splicing Detection Through Illumination Inconsistencies and Deep Learning", IEEE 2018

[3] Jason Bunk et al., "Detection and Localization of Image Forgeries Using Resampling Features and Deep Learning", IEEE 2017

[4] Clemens Seibold et al., "Detection of Face Morphing Attacks by Deep Learning", Springer 2017

[5] Yuan Rao ;JiangqunNiet, "A deep learning approach to detection of splicing and copy-move forgeries in images", IEEE 2016

[6] Belhassen Bayar, Matthew C. Stamm et al.,"A Deep Learning Approach to Universal Image Manipulation Detection Using a New Convolutional Layer", IEEE 2016.

[7] Jiansheng Chen ; Xiangui Kang ; Ye Liu ; Z. Jane Wang, "Median Filtering Forensics Based on Convolutional Neural Networks", IEEE 2015.

[8] Chi-Man Pun , Xiao-Chen Yuan , Xiu-Li Bi, "Image Forgery Detection Using Adaptive Oversegmentation and Feature Point Matching",IEEE 2015.

[9]Jian Li et al., "Segmentation-Based Image Copy-Move Forgery Detection Scheme", IEEE 2014

[10]DavideCozzolino ; Diego Gragnaniello ; Luisa Verdoliva, "Image forgery detection through residual-based local descriptors and block-matching", IEEE 2014

[11] GK Birajdar, VH Mankar, "Digital image forgery detection using passive techniques: A survey", Elsevier 2013

[12] G Lynch, FY Shih, HYM Liao, "An efficient expanding block algorithm for image copy-move forgery detection", Elsevier 2013

[13] M Hussain, G Muhammad, SQ Saleh, AM Mirza, "Image forgery detection using multi-resolution Weber local descriptors", IEEE 2013

[14] MF Hashmi, AR Hambarde, "Copy move forgery detection using DWT and SIFT features", IEEE 2013

[15] G Muhammad, M Hussain, G Bebis, "Passive copy move image forgery detection using undecimated dyadic wavelet transform", Elsevier 2012

[16] Gonzalez and Woods, "Digital Image processing", 2nd Edition, Person Publications.

