Hybrid Algorithm for Image Forgery Detection
Ms. Mansi R. Soni1 Ms.Kinjal N. Shah2 Mr. Shardul J. Agravat3
1P.G Student 2,3Assistant Professor
1,2,3Department of Computer Engineering
1,2Shri Pandit Nathulalji Vyas Technical Campus, India 3C U Shah College of Engineering and Technology, India

Abstract— Digital images are everywhere, on the covers of magazines, in news papers, in courtrooms, and all over the internet. But we cannot say that particular image is 100% authentic because it is possible that images can be manipulated. To manipulate or alter any image is known as Image forgery. There are number of techniques used for image forgery detection which are based on pixel, format, or source of given image. Proposed system will generate new approach of forgery detection method by combining two different techniques. One is based on LBP (Local binary pattern) method which gives good results for forgery detection. Another technique is based on Direction filter which shows that which portion of image has been forged. By combining these different techniques of forgery detection we will try to develop hybrid technique that will achieve good result for forgery detection.

Keywords: Image forensics, LBP, Direction filter, Forgery detection

I. INTRODUCTION

One of the simplest ways to develop a basic understanding of the extent of image processing applications is to categorize images according to their source. But if source image has been altered or manipulated then it is very difficult for viewer to judge the authenticity of a given image. Due to rapid advances and availabilities of powerful image processing software, it is easy to manipulate and modify digital images so it is necessary to check the authenticity of the image.

From the tabloid magazines to the fashion industry and in mainstream media outlets, scientific journals, political campaigns, courtrooms, and the photo hoaxes that land in our e-mail in-boxes, doctored photographs are appearing with a growing frequency and sophistication. Currently there are no established methodologies to verify the authenticity and integrity of digital images in an automatic manner.

Digital image forgery detection techniques are classified into active and passive approaches. In active approach, the digital image requires some pre-processing such as watermarking, signature etc at the time of creating the image. In passive approach, techniques work on the assumption that although digital forgeries may leave no visual clues that indicates tampering. Image forgery detection is a branch of image forensics which aims at assessing the authenticity and the origin of images. The existing image forensic tools can be generally classified into five categories which are:

1) Pixel-based techniques that detect statistical anomalies introduced at the pixel level.
2) Format-based techniques that leverage the statistical correlations introduced by a specific lossy compression scheme.
3) Camera-based techniques that exploit artifacts introduced by the camera lens, sensor, or on-chip post-processing.
4) Physically-based techniques that explicitly model and detect anomalies in the 3D interaction between physical objects, light, and the camera.
5) Geometric-based techniques that make measurements of objects in the world and their positions with respective to the camera.

II. RELATED WORK ON IMAGE FORGERY

Many passive approaches for image splicing forgery detection have been proposed so far. Previously some work has been done on these techniques. Splicing image forgery detection based on LBP and DCT have been done which achieves very good accuracy but this paper focusing on only splicing forgery [2]. Another method based on direction filter using JPEG analysis produce good result for image forgery detection. But this paper focusing on only copy-move forgery and images those have JPEG format because this method based on JPEG block analysis [1].

A. Local Binary Pattern (LBP):

LBP is a local operator which discriminates different types of textures. The original LBP operator defines a label (LBP code) of each pixel of an image. To compute the LBP code, a 3x3 neighborhood of the pixel is threshold by its intensity value. If the neighbor's pixel value is less than the center, it will hold binary digit '0', otherwise it will hold '1'. The neighbors' binary digits are concatenating to build a binary code. The LBP code is the decimal value of that binary code. When tampering is done, the original texture of the image is distorted. Due to the ability of LBP to capture the texture differences, it is an efficient tool for detection of the forgeries. Fig shows computation process of LBP.

B. Direction Filter Technique:

Direction Filter technique is based on Image edge detection and tampering localization. Image edge detection employs simple method of converting gray-level image into edge image. It is based on the fact that the tampered image region possesses high standard deviation surrounds the tampered region.

Fig. 1: Computation Process of LBP
For tampering localization Horizontal and Vertical projections are calculated and with the help of horizontal and vertical thresholds other directional edges are removed. Horizontal and Vertical edges images are combined together and feature map is generated. Feature Map is a binary image same size as original image where high intensity indicates possibility of tampering.

III. HYBRID ALGORITHM FOR IMAGE FORGERY DETECTION

All methods mentioned above are used to detect image forgery in different manner. Some methods are only give result that given image is forged or not and others are also used to display which portion of a given image is a forged portion.

In our hybrid algorithm, we combine both types of methods. One is LBP (Local binary pattern) that gives information about given image is forged or not and other method is based on direction filter technique that display which portion of image is forged[1][2].

A diagram of the proposed technique is shown in Fig. 3. First, the input RGB color images, one is original and second is tampered, are transformed to YCbCr color system.

![Fig. 2: YCbCr Component of Original Image](image)

These are preprocessing steps:
- Color space conversion
- Taking chrominance component of input images
- Division of Cb component image into overlapping block

Next, LBP is applied to each block and if result will give difference between input images then we can analyze from result that forgery has been present or not.

In next phase of our hybrid algorithm Direction filter technique is used to find out forged portion in given image if forgery has been detected from previous phase that has been used LBP method. At the end one feature map is generated that will describe the forged portion of given image.

![Fig. 3: Flowchart for Hybrid Algorithm](image)

IV. EXPERIMENT STRATEGY AND RESULT

By implementing first phase of given hybrid algorithm result of forgery has been analyzed and that is shown in following Fig. 4.

![Fig. 4: LBP Images of Original as Well as Tampered Image](image)

From result of above figure, it can be analyzed that forgery has been detected. If both input images are authenticate then it will not show difference in resulting LBP image. Next phase will be implemented only if forgery detected in previous phase. This phase is using direction filter technique.
for finding forged portion in given image. Final result of this hybrid algorithm will be look from following figures

The precision rate is defined as the ratio of correctly detected parts to the sum of correctly detected parts plus false positive. False positive are those regions in the image, which are actually not tampered parts, but have been detected by the algorithm as tampered parts.

\[
\text{Correctly detected parts} = \frac{\text{Correctly detected parts}}{\text{Correctly detected parts} + \text{False Positives}} \times 100\%
\]

The Recall rate is defined as the ratio of correctly detected parts to the sum of correctly detected parts plus false negatives. False negatives are those regions in the image, which are actually tampered parts, but have been not detected by the algorithm.

\[
\text{Recall Rate} = \frac{\text{Correctly detected parts}}{\text{Correctly detected parts} + \text{False Negatives}} \times 100\%
\]

Above equations have been used to predict Precision rate and Recall rate over various images those are available in our datasets. Table II explain this computation of Precision rate and Recall rate over different images considered from available datasets.

<table>
<thead>
<tr>
<th>Test Data</th>
<th>No. of Images</th>
<th>Precision Rate</th>
<th>Recall Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>CASIA1</td>
<td>100</td>
<td>94.6</td>
<td>94.8</td>
</tr>
<tr>
<td>Columbia</td>
<td>50</td>
<td>92.4</td>
<td>90.6</td>
</tr>
<tr>
<td>Total</td>
<td>150</td>
<td>93.5</td>
<td>92.7</td>
</tr>
</tbody>
</table>

Table-2: Computed Values of Precision Rate and Recall Rate On Given Datasets

V. CONCLUSION

In this paper Hybrid algorithm of image forgery detection has been developed that is based on LBP and Direction filter technique. This algorithm is not restricted to work on any particular type of forgery such as only copy-move image forgery or image splicing forgery. It shows that proposed features of chromatic channel are outperforming that of other color channel. The proposed method shows its consistency over CASIA TIDE v1.0, and Columbia datasets with average Precision rate and Recall rate of 93.5 and 92.7 respectively. These results are significantly better than other methods which are restricted to find any single type of forgery.

REFERENCES


for finding forged portion in given image. Final result of this hybrid algorithm will be look from following figures

![Figure 5: (a) Original image (b) Tampered image (c) Feature map](image_url)

1) Database:
The proposed method is evaluated using two benchmark databases: CASIA Tampered Image Detection Evaluation Database Version 1.0 (CASIA TIDE v1.0) and Columbia Uncompressed Image Splicing Detection evaluation Dataset.

<table>
<thead>
<tr>
<th>Dataset</th>
<th>No. of Images</th>
<th>Image Type</th>
<th>Image Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>CASIA1</td>
<td>800</td>
<td>jpg</td>
<td>384x256</td>
</tr>
<tr>
<td>Columbia</td>
<td>183</td>
<td>tif</td>
<td>757x568</td>
</tr>
<tr>
<td></td>
<td>180</td>
<td>bmp</td>
<td>1152x768</td>
</tr>
</tbody>
</table>

Table-1: Description of Evaluated Datasets

2) Evaluation Policy:
The precision and recall rates have been computed based on the number of correctly detected tampered parts in an image in order to evaluate the efficiency and robustness.


