A Novel method for Copy Move Blind Forgery Detection technique for Digital Image using DCT

Asif Hassan
Department of Electronics and Communication Engg.
Research Scholar, Bhagwant University
Rajasthan, India
asif.43hassan@gmail.com

Dr. V.K. Sharma
Department of Electronics and Communication Engg.
President/Vice-Chancellor, Bhagwant University
Rajasthan, India
viren_krec@yahoo.com

April 26, 2018

Abstract

Digital images are the integral part of our daily life. Images share information through newspapers, internet, and magazines. With ease of availability of image processing and editing tools, the image forgery has become common. Copy-move forgery is one of the many types of image forgery. In this type of forgery, a region of image is copied and pasted onto another region of the same image. This work proposes a novel method in which the image is divided into several overlapping blocks then the absolute value of Discrete cosine transform (DCT) of each block is calculated to extract feature of image. Finally the approximate mean value of each block is calculated and block matching method is used to identify the copied region.
1 INTRODUCTION

Digital image forgery detection methods are classified as active approach and passive approach as shown in Figure 1. Active approach requires some prior information of the image for forgery detection such as watermarking or signature. Passive approach does not require any prior information of image hence it is also known as “blind approach”.

In a Copy-Move forgery, a portion of the image is copied and pasted into another portion of the same image. This is done to hide an object in an image by wrapping it with a section copied from another part of the same image. The human eye cannot easily detect the suspicious objects as the copied parts come from the same image, its important properties will match with the rest of the image and hence will not be recognized.

![Figure 1: categories of image forgery detection](image)

The availability of image processing platforms, makes it easy to create Copy Move forgery. An example of a Copy Move forgery is shown in Figure 2.
There are many techniques have been proposed by various researchers to detect Copy Move Forgeries. Fridrich et al. [1] proposed a method in which the image is divided into overlapping blocks and DCT coefficients for feature extraction. Then, the similar blocks are detected and forged regions are found. Popescuet al. [2] proposed a technique for detecting small fixed-size image blocks using eigenvalues and Eigen vectors of each block and applying lexicographical sorting, the duplicate regions are automatically detected. Kang and Wei [3] proposed the use of SVD for extracting feature vector and dimension reduction then Lexicographical sorting is applied to detect forged regions. This algorithm is robust and efficient. Lin et al. [4] proposed a fast copy-move forgery detection technique for finding features vectors and dimension reduction then Radix sort is applied on feature vectors to detect forgery. Huang et al. [5] proposed the detection of copy-move forgery using SIFT algorithm using feature matching. Li et al. [6] proposed a method based on DWT and SVD and applied lexicographical sorting on singular value vector and the forged region is detected.

2 PROPOSED METHOD

The proposed method is to examine whether the input image contains copied regions or not and to identify the region from where it is copied from the same image. This method also tests the robustness of the algorithm for JPEG, BMP and TIF format images. The algorithm was tested for geometrical transformations like rotation. The proposed method is explained in the following steps. The color image or gray image of any pixel value is taken as input for which copy-move detection must be performed. The Color image is converted from RGB to Grey. Grey image is retained as it is.
input image is segmented into equal size overlapping blocks. The number of blocks depends on the size of the image. It is calculated using the equation Block size = 2^t, Where t = \log_2 (M \times N) - 12. Here ‘M’ is number of rows and ‘N’ is number of columns. The minimum pixel of image is considered as 128 \times 128. Hence minimum value of t is 2.

The number of overlapping blocks

\[ = \frac{M \times N}{\text{BlockSize}} \] (1)

Then calculate the absolute value of DCT for each Block. When the region is copied and rotated, the DCT value of the block will be negative making it difficult to find the similarity between the block. When we take the absolute value of DCT, we always end up with a positive number, which makes it easy to find the similarity between the block.

The Discrete Cosine Transform (DCT) helps separate the image into spectral sub-bands of differing importance with respect to the image’s visual quality. The DCT is similar to the Discrete Fourier transform. It transforms an image from the spatial domain to the frequency domain.

Calculate approximate value of mean of obtained DCT of each Block by using the following Formula

(Mean of test block X (1-\alpha) \leq \text{Mean of all blocks}) and

(Mean of test block X (1+\alpha) \geq \text{Mean of all blocks}) (2)

Then mean of each block is matched with all other possible overlapping blocks in the same image. If the similarity is found then the blocks are highlighted and considered as copied block.

3 SIMULATION AND RESULTS

The tests are carried out on the Mat Lab R2013A, a system with 2 GB RAM and 2.90 GHZ processor, the images with the different pixel values, saved in JPEG format. The images are tested to check the computational speed and robustness of the proposed algorithm. To evaluate performance of the copy move image forgery detection algorithm, simulation and results are performed on the Datasets:
COVERAGE [7] which contains copy-move forged (CMFD) images and their originals with similar but genuine objects (SGOs). COVERAGE is designed to highlight and address tamper detection ambiguity of popular methods, caused by self-similarity within natural images.

Figure 3a shows the Input image where the random rectangular region is copied and pasted onto the same image and Figure 3b shows the detected where the highlighted region represents the copied and pasted region. Figure 4a shows the Input image where the asymmetrical region is copied and pasted onto the same image and Figure 4b shows the detected where the highlighted region represents the copied and pasted region. The test is conducted without having prior knowledge (Blind approach) of the images with different pixel values.

The performance of the Proposed method to detect Copy Move Forgery is measured by True Positive Result (TPR), which correctly...
identifies the forged image and False Positive Result (FPR), which falsely identifies original image as forged image. The results are shown in Table I.

\[
T_{PR} = \frac{\text{forged imagedetected}}{\text{total forged image}} \times \%
\]

\[
F_{PR} = \frac{\text{original imagedetected forged}}{\text{total no. of original image}} \times \%
\]

TABLE I. TPR AND FPR IN PERCENTAGE

<table>
<thead>
<tr>
<th>Copy Move forgery type</th>
<th>TPR</th>
<th>FPR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rectangular region</td>
<td>99%</td>
<td>1%</td>
</tr>
<tr>
<td>Asymmetrical</td>
<td>99%</td>
<td>1%</td>
</tr>
</tbody>
</table>

The proposed method attained the accuracy of 99% for rectangular and Asymmetrical region Copy Move Forgery detection of images with different pixel size as shown in Table I.

4 Conclusion

The Proposed method is tested with a strong database. Irregular rectangular region Copy Move Forgery using MICC-F220 and for asymmetrical region Copy Move Forgery using CoMoFoD database. It is found that proposed work is robust for irregular rectangular region and asymmetrical region Copy Move Forgery. This method is effective for geometric transformations like scaling and rotation of copied region. The forgery is tested by means of DCT features and taking mean of DCT of blocks and comparing with other blocks of the same image. It works without any prior knowledge about the image (Blind approach). The proposed method is faster and more effective for any pixel size compared to existing methods.

References


