AN EFFICIENT IMAGE FORGERY DETECTION USING SIFT AND MIFT FEATURES

A. Jenefa Mariyal#
# PG Scholar, Computer Science and Engineering, Dr. Sivanthi Aditanar college of Engineering, Tiruchendur
jenefamariyal94@gmail.com

Abstract--- A copy–move forgery detection scheme using adaptive over segmentation and feature point matching is proposed in this project. The adaptive over segmentation algorithm segments the host image into non overlapping and irregular blocks adaptively. Then, the feature points are extracted from each block as block features, and the block features are matched with one another to locate the labeled feature points; this procedure can approximately indicate the suspected forgery regions.

SIFT (Scale invariant feature transform) is mostly used to match images but in case of flipped images it fails. A framework of mirror reflection invariant feature transform (MIFT) is used to overcome those failures.

Index Terms---- Copy-move forgery detection, adaptive over-segmentation, local color feature, forgery region extraction SIFT Features.

I. INTRODUCTION

Digital media like digital images and documents should be authenticated against the forgery due to the availability of powerful tools in the field of editing and manipulating these media. Digital imaging has matured to become the dominant technology for creating, processing, and storing pictorial memory and evidence. Though this technology brings many advantages, it can be used as a misleading tool for hiding facts and evidences. This is because today digital images can be manipulated in such perfection that forgery cannot be detected visually.

In fact, the security concern of digital content has arisen a long time ago and different techniques for validating the integrity of digital images have been developed. In the fields such as forensics, medical imaging, e-commerce, and industrial photography, authenticity and integrity of digital images is essential. In medical field physicians and researchers make diagnoses based on imaging. The introduction and rapid spread of digital manipulation to still and moving images raises ethical issues of truth, deception, and digital image integrity. With professionals challenging the ethical boundaries of truth, it creates a potential loss of public trust in digital media. This motivates the need for detection tools that are transparent to tampering and can tell whether an image has been tampered just by inspecting the tampered image. Image tampering is a digital art which needs understanding of image properties and good visual creativity. One tampers images for various reasons either to enjoy fun of digital works creating incredible photos or to produce false evidence. No matter whatever the cause of act might be, the forger should use a single or a combination series of image processing operations.

II. DETECTION METHODS

Block-Based Methods

In the existing block-based methods, the image is segmented into overlapping and regular image blocks. Then the forgery regions are identified by matching blocks of image pixels or transform coefficients. The existing algorithms use various techniques for forgery detection. These include Principal component Analysis (PCA), Discrete Cosine Transform (DCT), Discrete Wavelet Transforms (DWT), Singular Value Decomposition (SVD) etc. PCA is frequently used statistical technique for data dimension reduction. This method divides the image in multiple principal components to analyze different desired components. PCA based algorithms are applied in the areas of Image Color Reduction and Object Orientation. However, the major drawback of PCA is its insensitivity to relative scaling of the original variables. DCT works in frequency domain. It expresses a sequence of finitely data points in terms of a sum of cosine functions oscillating at different frequencies. DCT has numerous applications as in lossy compression of audio (e.g. MP3) and images (e.g. JPEG), image compression etc. However, DCT based methods do
not produce well results in case of image blurring and video frame reconstruction applications. DWT is wavelet transform for which the wavelets are discretely sampled. An approximation to DWT is used for data compression if signal is already sampled. It is an efficient approach to lossless compression. As compared to above methods, DWT has numerous drawbacks. Unlike PCA, DWT has high cost of computing. In contrast to DCT, DWT has certain limitations like signal blurring, ringing noise near edge regions in images or video frames, longer compression time, lower quality than JPEG at low compression rates etc. Another method called Singular Value Decomposition (SVD) is being increasingly used for tampering detection. SVD is a very robust technique. The technique involves refactoring of given digital image in three different feature based matrices. The small set called singular values preserve the useful features of the original image. The advantages of SVD include lesser memory requirement. It has many applications in data analysis, signal processing, pattern recognition, image compression, noise reduction, image blurring, face recognition, forensics, embedding watermarking to an image. Some techniques used Fourier-Mellin Transform (FMT) to obtain features.

Key point-Based Methods

An alternative to the block-based methods, key point-based forgery detection methods are proposed, where image key points are extracted and matched over the whole image to resist some image transformations while identifying duplicated regions. Two methods have been applied to achieve this, namely, the Scale-Invariant Feature transform (SIFT) and the Speeded up Robust Fatures (SURF). SIFT is applied to host images to extract feature points, which are then match to one another. When the value of the shift vector exceeded the threshold, the sets of corresponding SIFT feature points are defined as the forgery region. SURF is also applied to extract image feature instead of SIFT. Though these methods locate matched key points, most of them cannot detect forgery regions very well and therefore, the detection results are not so satisfactory and also the recall rate is low. Most of the block based forgery detection methods have similar framework, the difference being the method employed to extract the block features. Although these methods are effective they have three drawbacks. First, as the host image is divided into overlapping regular blocks, they become computationally expensive with increase in image size. Secondly, these methods cannot address significant geometrical transformations of the forged regions. Thirdly, their recall rate is low, since the blocking method is of regular shape. The key point based methods overcome the first two drawbacks, they reduce computational complexity and also successfully detect forgeries even when there are geometrical transformations, but the recall rate is very poor in these methods.

III.PROPOSED WORK

The development of computer technology and image processing software, digital image forgery has been increasingly easy to perform. During the copy and move operations, some image processing methods such as rotation, scaling, blurring, compression, and noise addition are occasionally applied to make convincing forgeries. Because the copy and move parts are copied from the same image, the noise component, color character and other important properties are compatible with the remainder of the image. Some of the forgery detection methods that are based on the related image properties are not applicable in previous case. Many forgery detection methods have been proposed for copy-move forgery detection. According to the existing methods, the copy-move forgery detection methods can be categorized into two main categories block-based algorithms and feature key point-based algorithms.

The existing block-based forgery detection methods divide the input images into overlapping and regular image blocks, then, the tampered region can be obtained by matching blocks of image pixels or transform coefficients. The proposed method in a forgery detection method in which the input image was divided into over-lapping rectangular blocks, from which the quantized Discrete Cosine Transform (DCT) coefficients of the blocks were matched to find the tampered regions.
1. Adaptive Over Segmentation

This step segments the host image into non-overlapping irregular blocks. It is similar to traditional block-based forgery detection methods. In the existing block-based detection schemes, the host image is usually divided into overlapping regular blocks, with the block size defined and fixed beforehand. Then, the forgery regions are detected by matching those blocks. Due to the regular shape of the blocks, the recall rate of these methods is low. Also, as the size of the host image increases, the matching computation of the overlapping blocks will be much expensive. To divide the host image into non-overlapping regions of irregular shape which are perpetually meaningful atomic regions, Simple Linear Iterative Clustering (SLIC) algorithm is used. It adapts k-means clustering approach to efficiently generate the super pixels. But, the initial size of the super pixels in SLIC is difficult to decide. If the initial size of the super pixels is too small, the result will be a large computational expense and if it is too large, the forgery detection results are not significantly accurate. Therefore, a balance between the computational expense and the detection accuracy must be obtained when employing the SLIC segmentation method for image blocking. In this proposed work, an Adaptive over-segmentation is used which determines the initial block size based on the texture of the host image. When the texture of the image is smooth, the initial size of the super pixels is relatively large, which can ensure not only that the super pixels will get close to the edges, but also will contain sufficient feature points to be used for forgery detection. Also, larger super pixels imply a smaller number of blocks, which can reduce the computational expense when the blocks are matched with each other. In contrast, when the texture of the host image has more detail, then the super pixel size is relatively small, to ensure good forgery detection results.

1.1 Discrete Wavelet Transform (DWT)

The Discrete wavelet Transform (DWT) is used to analyze the frequency distribution of the host image. Roughly, when low-frequency energy accounts for the majority of the frequency energy, the image will appear to be smooth; otherwise, if the low-frequency energy accounts for only a minority of the frequency energy, the host image appears to be a detailed image. In this proposed work, four-level DWT is performed, using the ‘Haar’ wavelet, on the host image to calculate the low-frequency energy and high-frequency energy.

First the DWT is employed to the host image to obtain the coefficients of the low- and high-frequency sub-bands of the host image. Then, calculate the percentage of the low-frequency distribution $PLF$ to determine the initial size $S$. Finally, employ the SLIC segmentation algorithm together with the calculated initial size $S$ to segment the host image to obtain the image blocks (IB).

1.2 SLIC Segmentation

SLIC (Simple Linear Iterative Clustering) clusters pixels based on their color similarity and proximity in the image plane. It performs a local clustering of pixels in 5-D space defined by the L, a, b values of the CIELAB color space and x, y coordinates of the pixels. SLIC takes a desired number of approximately equally-sized super pixels k as input. It begins by sampling k regularly spaced cluster centers and moving them to seed locations corresponding to the lowest gradient position in a $3 \times 3$ neighborhood. Each pixel in the image is associated with the nearest cluster center whose search area overlaps this pixel. After all the pixels are associated with the nearest cluster center, a new center is computed as the average laxly vector of all the pixels belonging to the cluster. The assignment and update steps are repeated iteratively until the error converges. Finally, a post-processing step enforces connectivity by reassigning disjoint pixels to nearby super pixels. Copy-move forgery as depicted usually means that part of the images paste. However, people easily modify the geometry of the copied part so that the forged image seems to be original. Among the geometric modifications, rotation is commonly used to provide spatial synchronization between the copied region and its neighbors. In this work, therefore, the forgery technique which copies a region and rotates it before pasting is named as copy-rotate-move (CRM) forgery.

The clustering procedure begins with an initialization step where k initial cluster centers Ci
2 Block Feature Extraction Algorithm

After the host image is segmented into image blocks, block features are extracted from the image blocks (IB). The traditional block-based forgery detection methods extracted features of the same length as the block features or directly used the pixels of the image block as the block features. However, these features reflect mainly the content of the image blocks, leaving out the location information. Also, these features are not resistant to various image transformations. Therefore, in this work, the feature points are extracted from each image block as block features and the feature points should be robust to various distortions, such as image scaling, rotation, and JPEG compression. The feature point extraction methods, SIFT and SURF have been widely used. The feature points generated using these methods are robust against common image processing operations such as rotation, scale, blurring, and compression. Experiments have shown that the results obtained using SIFT [2] are more constant and have better performance compared to other feature extraction methods. Hence, in this work SIFT is used for feature point extraction. Therefore, each block feature contains irregular block region information and the extracted SIFT feature points.

2.1 Scale Invariant Feature Transform (SIFT)

SIFT extracts key points and computes its descriptors. It involves four main steps which are explained below.

Step 1: Scale-Space Extreme Detection
Scale-space filtering is used in this step. Difference of Gaussian is obtained as the difference of Gaussian blurring of an image with different σ values. This process is done for different octaves of the image in Gaussian pyramid. Next, the images are searched for local extreme over scale and space. If it is the local extreme, it is a potential key point.

Step 2: Key point Localization
Once potential key points locations are found, they are refined to get more accurate results. Taylor series expansion of scale space is used to get more accurate location of extreme, and if the intensity at this extreme is less than a threshold value, it is rejected. This threshold is called contrast Threshold. DoG has higher response for edges, so edges also needed to be removed. For this, a concept similar to Harris corner detector is used. A 2x2 Hessian matrix (H) is used to compute the principal curvature. For edges, one Eigen value is larger than the other. So here they used a simple function, if this ratio is greater than a threshold, called edge Threshold, that key point is discarded. So it eliminates any low-contrast key points and edge key points and what remain is strong interest points.

Step 3: Orientation Assignment
One or more orientations are assigned to each key point location based on local image gradient directions. A neighborhood is taken around the key point location depending on the scale, and the gradient magnitude and direction is calculated in that region. An orientation histogram with 36 bins covering 360 degrees is created. (It is weighted by gradient magnitude and Gaussian-weighted circular window with σ equal to 1.5 times the scale of key point. The highest peak in the histogram is taken and any peak above 80% of it is also considered to calculate the orientation. It creates key points with same location and scale, but different directions. It contributes to stability of matching.

Step 4: Key point Descriptor
A 16x16 neighbourhood around the key point is taken. It is divided into 16 sub-blocks of 4x4 size. For each sub-block, 8 bin orientation histogram is created. So a total of 128 bin values are available. It is represented as a vector to form key point descriptor.

2.2 Mirror Reflection Invariant Feature Transform (MIFT)

The various approaches explained in literature survey for key point based forgery detection fails for reflective images. The FPR and time taken is high, also accuracy is low. These problems can be resolved by combining the Lowe’s SIFT with Irene’s contribution and improvising it with X. Guo’s MIFT. The following sections explore all these approaches.

Lowe’s SIFT

Various images can be obtained with the help of appropriate approach as quality of image differentiate from one another. As a result this differentiation can be used for object recognition. The steps used for finding the descriptors are as follows.

Step 1: Scale-Space Extreme Detection

The first stage of computation searches over all scales and image locations. It is implemented efficiently by using a difference-of-Gaussian (DoG).

Step 2: Keypoint Localization

Each point of an image is identified by its location and quality. Key points are determined from these specifications.

Step 3: Orientation Assignment

One or more orientations are assigned to each key point location based on local image gradient directions. Post-processing is done to remove the effect of transformations.

Step 4: Keypoint Descriptor

The slope is computed at predetermined scale around key points. Then they are represented into a 128 bit array.

3. Block Feature Matching Algorithm

After the block features (BF) are obtained locate the matched blocks through the block features. In most of the existing block-based methods, the block matching process outputs a specific block pair only if there are many other matching pairs in the same mutual position, assuming that they have the same shift vector. When the shift vector exceeds a user-specified threshold, the matched blocks that contributed to that specific shift vector are identified as regions that might have been copied and moved. In the proposed algorithm, because the block feature is composed of a set of feature points a different method is adapted to locate the matched blocks. First, the number of matched feature points is calculated, and the correlation coefficient map is generated, then the corresponding block matching threshold is calculated adaptively with the result, the matched block pairs are located; and finally, the matched feature points in the matched block pairs are extracted and labeled to locate the position of the suspected forgery region.

Input: Block Features (BF).
Output: Labeled Feature Points (LFP).

STEP-1: Load the Block Features \( BF = \{BF_1, BF_2, \ldots, BF_N\} \), where \( N \) means the number of image blocks; and calculate the correlation coefficients \( CC \) of the image blocks.

STEP-2: Calculate the block matching threshold \( T_{RB} \) according to the distribution of correlation coefficients.

STEP-3: Locate the matched blocks \( MB \) according to the block matching threshold \( T_{RB} \).

STEP-4: Label the matched feature points in the matched blocks \( MB \) to indicate the suspected forgery regions.

4. Forgery Region Extraction Algorithm

Although the labeled feature points (LFP) are extracted, which are only the locations of the forgery regions, still locate the forgery regions. Considering that the super pixels can segment the host image very well, a method is proposed by replacing the LFP with small super pixels to obtain the suspected regions (SR), which are combinations of labeled small super pixels.

Furthermore, to improve the precision and recall results, measure the local color feature of the super pixels that are neighbors to the suspected regions (SR); if their color feature is similar to that of the suspected regions, then we merge the neighbor super pixels into the corresponding suspected regions, which generates the merged regions (MR). Finally, a close morphological operation is applied to the merged regions to generate the detected copy-move forgery regions.

Input: Labeled Feature Points (LFP)
Output: Detected Forgery Regions.
STEP-1: Load the Labeled Feature Points (LFP), apply the SLIC algorithm with the initial size $S$ to the host image to segment it into small super pixels as feature blocks, and replace each labeled feature point with its corresponding feature block, thus generating the Suspected Regions (SR).

STEP-2: Measure the local color feature of the super pixels neighbor to the SR, called neighbor blocks; when their color feature is similar to that of the suspected regions, merge the neighbor blocks into the corresponding SR, therefore creating the merged regions (MR).

STEP-3: Apply the morphological close operation into MR to finally generate the detected forgery regions.

Table 1. Comparison of SIFT and MIFT

<table>
<thead>
<tr>
<th>Method</th>
<th>SIFT</th>
<th>MIFT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database</td>
<td>MCCI, F2000</td>
<td>CASIA</td>
</tr>
<tr>
<td>Tempered Images</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>Non Tempered Images</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>TP</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>TN</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>FN</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IPR (%)</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FPR (%)</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Accuracy (%)</td>
<td>100</td>
<td>100</td>
</tr>
</tbody>
</table>

IV. CONCLUSION

Digital forgery images created with copy-move operations are challenging to detect. In this work copy-move forgery detection scheme using adaptive over-segmentation and feature-point matching is proposed. The Adaptive over-segmentation algorithm is proposed to segment the host image into non-overlapping and irregular blocks adaptively according to the given host images using this approach, for each image, determine an appropriate block initial size to enhance the accuracy of the forgery detection results and, at the same time, reduce the computational expenses. Then, in each block, the feature points are extracted as block features, and the block features are matched with one another to locate the labeled feature points using Block Feature Matching Algorithm this procedure can approximately indicate the suspected forgery regions. Subsequently, to detect the more accurate forgery regions, the labeled feature points are replaced with small super pixels as feature blocks, and the neighboring feature blocks with local color features that are similar to the feature blocks are merged to generate the merged regions by the Forgery Region Extraction algorithm. The morphological operation is applied to the merged regions to generate the detected forgery regions.

V. REFERENCES