ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 3, March 2016

6th International Conference in Magna on Emerging Engineering Trends 2016 [ICMEET 2016]
On 10th & 11th March, 2016
Organized by
Dept. of ECE, EEE & CSE, Magna College of Engineering, Chennai-600055, India.

Image Forgery Detection Using Feature Point Matching

A.Maria Venitta, V.Sheeja Kumari

PG Student, Department of CSE, Rajas Engineering College, Vadakkangulam, Tamil Nadu, India

Assistant Professor, Department of CSE, Rajas Engineering College, Vadakkangulam, Tamil Nadu, India

ABSTRACT: A novel copy–move forgery detection scheme using adaptive over segmentation and feature point matching is proposed in this paper. The proposed scheme integrates both block-based and key point-based forgery detection methods. First, the proposed 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. To detect the forgery regions more accurately, we propose the forgery region extraction algorithm, which replaces the feature points with small super pixels as feature blocks and then merges the neighboring blocks that have similar local color features into the feature blocks to generate the merged regions. Finally, it applies the morphological operation to the merged regions to generate the detected forgery regions. The experimental results indicate that the proposed copy–move forgery detection scheme can achieve much better detection results even under various challenging conditions compared with the existing state-of-the-art copy–move forgery detection methods.

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.

Forgery techniques
The various commonly used image tampering techniques are as follows.

Copy-move

This is the most common kind of image tampering technique used, where one needs to cover a part of the image in order to add or remove information. Textured regions are used as ideal parts for copy-move forgery. Since textured areas have similar color, dynamic range, noise variation properties to that of the image, it will be unperceivable for human eye investigating for incompatibilities in image statistical properties.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 3, March 2016

6th International Conference in Magna on Emerging Engineering Trends 2016 [ICMEET 2016]
On 10th & 11th March, 2016
Organized by
Dept. of ECE, EEE & CSE, Magna College of Engineering, Chennai-600055, India.

Image-splicing

It is defined as a paste-up produced by sticking together photographic images. Splicing is a technique which involves composite of two or more images to create a new fake image.

Resize

This operation performs a geometric transformation which can be used to shrink or enlarge the size of an image or part of an image. Image reduction is performed by interpolating between pixel values in local neighborhoods.

Cropping

It is a technique to cut-off borders of an image or reduces the canvas on which an image is displayed. Generally this kind of operation is used to remove border information which is not very important for display.

Noising or Blurring

Tampering images with operations described above like image splicing, scaling, rotating can be clear to a viewer in the form of artifacts like improper edges, aliasing defects and tone variations. These obvious traces of tampering can be made imperceptible by applying small amount of noise or blur operations in the portions where the tampering defects are visible.This project focuses on copy-move forgery, that can be done very easily by using the tools such as Cloning in Photoshop. In this type of tampering, portions of an image are copied and pasted in other portions of the same image to conceal a person or object in the scene. Fig. 1 shows an example of copy-move forgery where the leaves are duplicated to hide a vehicle from the image.

Fig.1. Left is the original, right is the tampered image

Because the copy and move parts are from the same image, the noise component , color character and other 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 this case.

Detection Methods

The copy-move forgery detection methods fall under two main categories: block-based algorithms and feature keypoint-based algorithms.

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

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 3, March 2016

6th International Conference in Magna on Emerging Engineering Trends 2016 [ICMEET 2016]
On 10th & 11th March, 2016
Organized by
Dept. of ECE, EEE & CSE, Magna College of Engineering, Chennai-600055, India.

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.

Keypoint-based methods

An alternative to the block-based methods, keypoint-based forgery detection methods are proposed, where image keypoints 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 Fetures (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 keypoints, 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 keypoint 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.

II. EXISTING METHODS AND SYSTEM ANALYSIS

LITERATURE SURVEY

2.1 Detecting Duplicated Image

Alin C Popescu et al.(2004) proposed a technique that works by first applying principal component analysis to small fixed-size image blocks to yield a reduced dimension representation. Duplicated regions are then detected by lexicographically sorting all of the image blocks. This technique is effective on plausible forgeries, and have quantified its sensitivity to JPEG lossy compression and additive noise. Detection is possible even in the presence of significant amounts of corrupting noise using this method.

2.2 Fast Copy-Move Forgery Detection

Hwei-jen lin et.al (2009) have proposed a method to detect copy- move forgery by dividing the image into overlapping blocks of equal size, extracting feature for each block and representing it as a vector and sorting all the extracted feature vectors using the radix sort. Radix sort dramatically reduces the time complexity and the adopted features enhance the capability of resisting of various attacks such as JPEG compression and Gaussian noise. Both efficiency and high detection rates have been demonstrated. A few small copied regions were not successfully detected. Although duplicated regions with rotation through some fixed angles can be detected, this method does not deal with rotation arbitrary angles.

2.3 Robust Copy-move Forgery

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 3, March 2016

6th International Conference in Magna on Emerging Engineering Trends 2016 [ICMEET 2016]
On 10th & 11th March, 2016
Organized by
Dept. of ECE, EEE & CSE, Magna College of Engineering, Chennai-600055, India.

Sevinc Bayram et al.(2009) proposed to use Fourier-Mellin Transform (FMT) features which are invariant to scaling and translation. They also presented a new detection scheme that make use of counting bloom filters. It detects copy-move forgery very accurately even if the forged image is rotated, scaled or highly compressed. This detection scheme improves the efficiency, but the robustness of the method is reduced.

2.4 Fast and Robust Image Region

WANG Jun-Wen et.al. (2009) proposed an algorithm to detect region-duplication forgery where the image is first reduced in dimension by Gaussian pyramid, and the Hu moment is applied to the fixed sized overlapping blocks of low-frequency image. The eigenvectors are lexicographically sorted. Then, similar eigenvectors are matched by a certain threshold value. Finally, the area threshold value is proposed to remove the wrong similar blocks. This method is robust and it can not only successfully detect this type of tampering for images subject to various forms of post region duplication image processing, including noise contamination, blurring, and severe lossy compression, but also reduce the total number of blocks to narrow block-matching searching space, which can improve the method efficiency. The detection rate of this method is low and also it works only within same image and does not work between different images.

2.5 Region detection Using Image Feature Matching

Xunyu Pan et al. (2010) proposed a method for region duplication detection by estimating the transform between matched SIFT keypoints and then finding the duplicated regions after discounting the estimated transforms. It is effective even when the duplicated regions are distorted. SIFT algorithm cannot find the reliable keypoints in regions with little visual structures. Also, smaller regions having fewer keypoints hard to detect. Images having intrinsically identical regions cannot be differentiated from intentionally duplicated regions.

2.6 Detection Digital Images Using SURF

B.L.Shivakumar et al. (2011) proposed a method that detects the duplication region using SURF keypoints which are extracted from the images. It detects duplication region with different size. The result shows that the proposed method can detect copy-move forgery with minimum false match for images with high resolution. A few small copied regions were not successfully detected.

2.7 A Sift-based Forensic Method

Irene Amerini et al. (2011) proposed a methodology to support image forensics investigation based on SIFT features. It can reliably detect if a certain region has been duplicated and, determine the geometric transformation applied to perform such tampering. In a cloned image patch with highly uniform texture, salient keypoints are not recovered by SIFT-like techniques.

2.8 Exposing Transform-invariant Features

Pravin Kakar et al.(2012) have proposed a method based on transform-invariant features. These obtained y using the features from MPEG-7 image signature tools. These features display good accuracy and extremely low false positives. It has achieved good results as these descriptors are invariant to common image processing operations. This method cannot detect regions which have undergone affine transformations and/or multiply copied.

2.9 SLIC Superpixels Methods

Radhakrishna Achanta et al. (2012) have proposed a in-depth performance analysis of modern superpixel techniques. They performed an empirical comparison of five state-of-the-art algorithms. In addition, it proposed a new method for generating superpixels based on k-means clustering, SLIC, which has been shown to outperform existing superpixel methods . SLIC adheres to boundaries as well as or better than previous methods. At the same time, it is faster and more memory efficient, improves segmentation performance.

2.10 Evaluation of Popular Copy-Move

Vincent Christlein et.al. (2012) have analyzed various copy-move forgery detection algorithms and answered which algorithm perform best in various post processing scenarios. The keypoint-based method, e.g based on SIFT features,

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 3, March 2016

6th International Conference in Magna on Emerging Engineering Trends 2016 [ICMEET 2016]
On 10th & 11th March, 2016
Organized by
Dept. of ECE, EEE & CSE, Magna College of Engineering, Chennai-600055, India.

can be very efficiently executed. Its main advantage is the remarkably low computational load, combined with good performance. Keypoint-based methods, however, are sensitive to low-contrast regions and repetitive image content. Here, block-based methods can clearly improve the detection results. Copy-move forgery as depicted means that the copied part of the image is pasted into another part of the image without any geometric change. However , people easily modify the geometry of the copied part so that the forged image seems to be original.

2.11 Existing System

Traditional system used block based forgery detection and feature matching algorithm separately .In previous years, many forgery detection methods have been proposed for copy-move forgery detection. According to the existing methods, the copy-move forgery detection method scan 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.Most of the existing block-based forgery detection algorithms use a similar framework, and the only difference is that they apply different feature extraction methods to extract the block features. . Although the existing keypoint-based forgery detection methods can avoid computational complexity and can successfully detect the forgery, even when some attacks exist in the host images; the recall results of the existing keypoint-based forgery methods were very poor.From which the quantized Discrete Cosine Transform (DCT) coefficients of the blocks were matched to find the tampered regions. Popescu and Farid applied Principal Component Analysis (PCA) to reduce the feature dimensions.Luoet al. [used the RGB color components and direction information as block features. Li et al. Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) to extract the image features. Mahdian and Saic calculated the 24 Blur-invariant moments as features. Kang and Wei calculated the singular values of a reduced-rank approximation in each block. Bayram et al. used the Fourier-Mellin Transform (FMT) to obtain features. Wang et al. The mean intensities of circles with different radii around the block center to represent the block features.Lin et al. used the gray average results of each block and its sub-blocks as the block features. Ryu et al. Zernike moments as block features. Bravo-Solorio and Nandi used information entropy as block features. As an alternative to the block-based methods, key point based forgery detection methods were proposed, where image key points are extracted and matched over the whole image to resist some image transformation while identifying duplicated regions.

In Scale-Invariant Feature Transform (SIFT) was applied to the host images to extract feature points, which were then matched to one another. When the value of the shift vector exceeded the threshold, the sets of corresponding SIFT feature points were defined as the forgery region. However, although these methods can locate the matched key points, most of them cannot locate the forgery regions very well; therefore, they cannot achieve satisfactory detection results and, at the same time, a sustained high recall rate . Most of the existing block-based forgery detection algorithms use a similar framework, and the only difference is that they apply different feature extraction methods to extract the block features.

Disadvantages

- The host image is divided into over-lapping rectangular blocks, which would be computationally expensive as the size of the image increases.
- The method cannot address significant geometrical transformations of the forgery regions
- Their recall rate is low because their blocking method is regular shape.

2.12 PROPOSED SYSTEM

This paper propose, a novel copy-move forgery detection scheme using adaptive over-segmentation and feature point matching. The proposed scheme integrates both the traditional block-based forgery detection methods and key point-based forgery detection methods. Similar to block-based forgery detection methods, we propose an image-blocking method called the Adaptive Over-Segmentation algorithm to divide the host image into non-overlapping and irregular blocks adaptively. Then, similar to the keypoint-based forgery detection methods, the feature points are extracted from each image block as block features instead of being extracted from the whole host image as in the traditional key point-base methods. Subsequently, the block features are matched with one another to locate the labeled feature points, which can approximately indicate the suspected forgery regions.To detect more accurate forgery regions, we proposed the Forgery Region Extraction algorithm, which replaces the feature points with small super pixels as feature blocks and,

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 3, March 2016

6th International Conference in Magna on Emerging Engineering Trends 2016 [ICMEET 2016]
On 10th & 11th March, 2016
Organized by
Dept. of ECE, EEE & CSE, Magna College of Engineering, Chennai-600055, India.

then, merges the neighboring blocks with similar local color features into feature blocks, to generate the merged regions; finally, it applies a morphological operation into the merged regions to generate the detected forgery regions.

Adaptive over segmentation divide the image into non-overlapping and irregular blocks .The latter extracts feature points from each block as block features and the block features are matched with one another to locate labeled feature points. This approximately determines the forgery regions. proposed 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.The RGB color components and direction information as block features. As an alternative to the block-based methods, key point based forgery detection methods were proposed, where image key points are extracted and matched over the whole image to resist some image transformations while identifying duplicated regions. The Scale-Invariant Feature Transform (SIFT) was applied to the host images to extract feature points ,which were then one another.

Advantages:

- Yields better results when compared to the earlier techniques.
- Segments the host image into non-overlapping and irregular blocks adaptively.

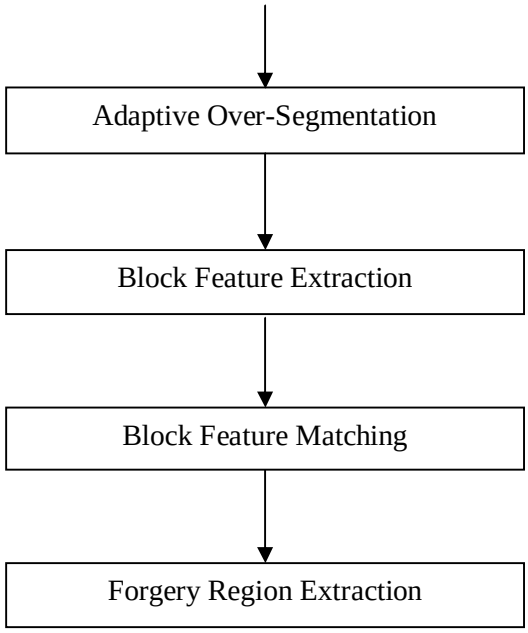

Fig 2. Block diagram of proposed system

2.13 MODULES DESCRIPTION

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 superpixels. But, the initial size of the superpixels in SLIC is difficult to decide. If the initial

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 3, March 2016

6th International Conference in Magna on Emerging Engineering Trends 2016 [ICMEET 2016]
On 10th & 11th March, 2016
Organized by
Dept. of ECE, EEE & CSE, Magna College of Engineering, Chennai-600055, India.

size of the superpixels 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 project, 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 superpixels is relatively large, which can ensure not only that the superpixels will get close to the edges, but also will contain sufficient feature points to be used for forgery detection. Also, larger superpixels 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 superpixel size is relatively small, to ensure good forgery detection results. 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 project, four-level DWT is performed, using the 'Haar' wavelet, on the host image to calculate the low-frequency energy E_{LF} and high-frequency energy E_{HF} using (1) and (2) and then the percentage of the low-frequency distribution P_{LF} is calculated using (3), according to which the initial size S of the superpixels is defined as in (4).

$$E_{LF} = \sum |CA_4| E_{HF} = \sum_i (\sum |CD_i| + \sum |CH_i| + \sum |CV_i|) \quad i = 1,2,....,4$$

where CA_4 indicates the approximation coefficients at the 4^{th} level of DWT , and CD_i , CH_i and CV_i indicate the detailed coefficients at the i^{th} level of DWT, i = 1,2,...,4.

$$P_{LF} = \frac{E_{LF}}{E_{LF} + E_{HF}} .100\%$$

$$S = \begin{cases} \sqrt{0.02 \times M \times N}\, P_{LF} > 50\% \\ \sqrt{0.01 \times M \times N} P_{LF} \leq 50\% \end{cases}$$

where S means the initial size of the superpixels , M x N indicates the size of the host image and P_{LF} means the percentage of the low-frequency distribution.

Finally, the SLIC segmentation algorithm together with the calculated initial size S is employed to obtain the image blocks (IB). The flowchart of Adaptive Over-Segmentation is shown in Fig.2.

2.14 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 colorspace and x, y coordinates of the pixels. SLIC takes a desired number of approximately equally-sized superpixels 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 × 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 superpixels. 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 paper, therefore, the forgery technique which copies a region and rotates it before pasting is named as copy-rotate-move (CRM) forgery. SLIC is simple to use and understand. By default, the only parameter of the algorithm is k, the desired number of approximately equally sized superpixels. For color images in the CIELAB color space, the clustering procedure begins with an initialization step where k initial cluster centers Ci ¼½ li ai bi xi yiT are sampled on a regular grid spaced S pixels apart. To produce roughly equally sized superpixels, the grid interval N=kp. The centers are moved to seed locations corresponding to the lowest gradient position in a neighborhood. This is done to avoid centering a superpixel on an edge and to reduce the chance of seeding a superpixel with a noisy pixel.

Next, in the assignment step, each pixel i is associated with the nearest cluster center whose search region overlaps its location. This is the key to speeding up our algorithm because limiting the size of the search region significantly

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 3, March 2016

6th International Conference in Magna on Emerging Engineering Trends 2016 [ICMEET 2016]
On 10th & 11th March, 2016
Organized by
Dept. of ECE, EEE & CSE, Magna College of Engineering, Chennai-600055, India.

reduces the number of distance calculations, and results in a significant speed advantage over conventional k-means clustering where each pixel must be compared with all cluster centers. This is only possible through the introduction of a distance measure D, which determines the nearest cluster center for each pixel. Since the expected spatial extent of a superpixel is a region of approximate size S, the search for similar pixels is done in a region 2S around the superpixel center. Once each pixel has been associated to the nearest cluster center, an update step adjusts the cluster centers to be the mean ½labxy vector of all the pixels belonging to the cluster. The L2 norm is used to compute a residual error E between the new cluster center locations and previous cluster center locations. The assignment and update steps can be repeated iteratively until the error converges, but we have found that 10 iterations suffices for most images, and report all results in this paper using this criteria. Finally, a post processing step enforces connectivity by reassigning disjoint pixels to nearby super pixel.

2.15 Block Feature Extraction

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 project, 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 are more constant and have better performance compared to other feature extraction methods. Hence, in this project SIFT is used for feature point extraction. Therefore, each block feature contains irregular block region information and the extracted SIFT feature points.

2.16 Scale Invariant Feature Transform (SIFT)

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

Step1 : Scale-space extrema 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 extrema over scale and space.If it is the local extrema, it is a potential keypoint.

Step 2 : Keypoint localization

Once potential keypoints locations are found, they have are refined to get more accurate results. Taylor series expansion of scale space is used to get more accurate location of extrema, and if the intensity at this extrema is less than a threshold value, it is rejected. This threshold is called contrastThreshold . DoG has higher response for edges, so edges also need to be removed. For this, a concept similar to Harris corner detector is used. A 2x2 Hessian matrix (H) is used to compute the pricipal 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 edgeThreshold , that keypoint is discarded. So it eliminates any low-contrast keypoints and edge keypoints and what remains is strong interest points.

Step 3 : Orientation assignment

One or more orientations are assigned to each keypoint location based on local image gradient directions. A neighborhood is taken around the keypoint 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 keypoint. The highest peak in the histogram is taken and any peak above 80% of it is also considered to calculate the orientation. It creates keypoints with same location and scale, but different directions. It contribute to stability of matching.

Step 4: Keypoint Descriptor

A 16x16 neighbourhood around the keypoint is taken. It is devided 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 keypoint descriptor.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 3, March 2016

6th International Conference in Magna on Emerging Engineering Trends 2016 [ICMEET 2016]

On 10th & 11th March, 2016

Organized by

Dept. of ECE, EEE & CSE, Magna College of Engineering, Chennai-600055, India.

IV. EXPERIMENTAL RESULTS ANDDISCUSSIONS

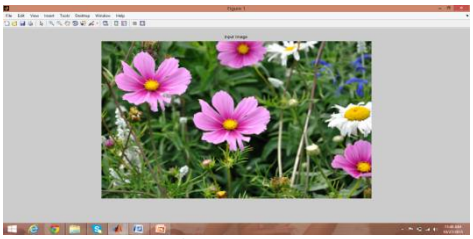

Fig 3. Input Image

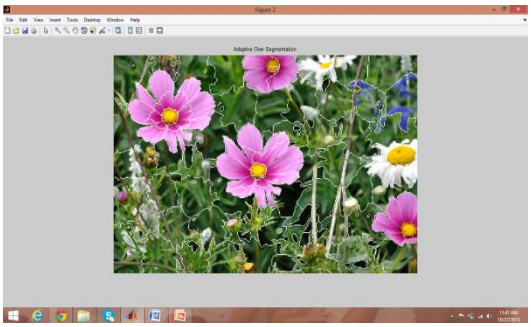

Fig 4. Segmented by Adaptive overlap Image

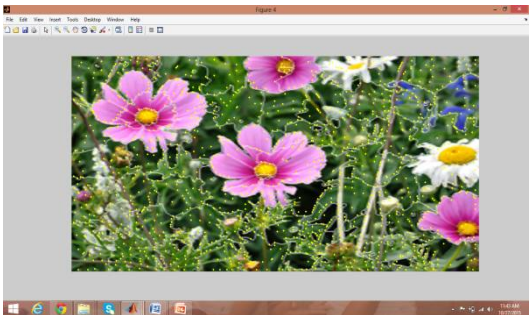

Fig 5. Future Point Extraction

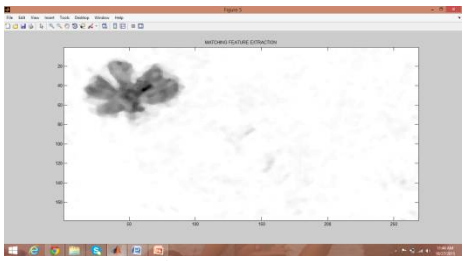

Fig 6. Forgery Image

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 3, March 2016

6th International Conference in Magna on Emerging Engineering Trends 2016 [ICMEET 2016]
On 10th & 11th March, 2016
Organized by
Dept. of ECE, EEE & CSE, Magna College of Engineering, Chennai-600055, India.

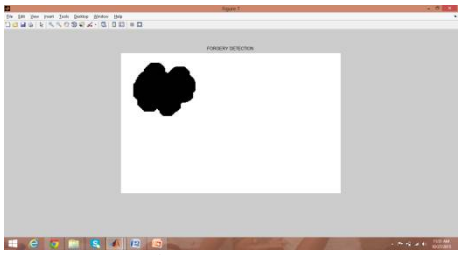

Fig 6. Forgery Region

V. CONCLUSION

In contrast of block –based algorithms and key point based algorithms, and feature point matching detects the forgery region more accuracy overcomes the drawbacks of the existing methods. Digital forgery images created with copy-move operations are challenging to detect. In this paper, we have proposed a novel copy-move forgery detection scheme using adaptive over-segmentation and feature-point matching. 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, we can 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 Feature Matching algorithm is proposed, with which the block features are matched with one another to locate the labeled feature points.

REFERENCES

[1] J. Fridrich, D. Soukal, and J. Lukáš , “Detection of copy–move forgery in digital images,” in Proc. Digit. Forensic Res. Workshop, Cleveland, OH, Aug. 2003.
[2] A. C. Popescu and H. Farid, “Exposing digital forgeries by detecting duplicated image regions,” Dept. Comput. Sci. NH, USA, Tech. Rep. TR2004-515, 2004.
[3] W. Luo, J. Huang,“ Detection of region-duplication of image,”Proc. 18th Pattern Recognit. (ICPR), Aug. 2006.
[4] G. Li, Q. Wu, D. Tu, and S. Sun, “A sorted neighborhood approach for detecting region , in Proc. IEEE Int. Conf. Multimedia Expo, Jul. 2007, pp. 1750–1753.
[5] B. Mahdian and S. Saic, “Detection of copy–move forgery using a method based on moment invariants,” Forensic Sci. Int., vol. 171, nos. 2–3, pp. 180–189, 2007.
[6] X. B. Kang and S. M. Wei, “Identifying tampered regions using singular value decomposition in digital image forensics,” in Proc. Int. Dec. 2008, pp. 926–930.
[7] S. Bayram, H. T. Sencar,“An efficient and robust method for copy–move forgery,” in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP), Apr. 2009, pp. 1053–1056.
[8] J. Wang, G. Liu, H. Li, Y. Dai, and Z. Wang, “Detection of image region duplication forgery using model with circle block,” in Proc. Int. Conf. Multimedia Inf. Netw. Secur. (MINES), Nov. 2009, pp. 25–29.
[9] J. W. Wang, G. J. Liu, Z. Zhang, Y. W. Dai, and Z. Q. Wang, “Fast and robust forensics for image region-duplication forgery,” Acta Automat. Sinica, vol. 35, no. 12,
[10] H. J. Lin, C. W. Wang, and Y. T. Kao, “Fast copy–move forgery detection,” WSEAS Trans. Signal Process., vol. 5, no. 5, pp. 188–197, 2009.
[11] S. J. Ryu, M. J. Lee, and H. K. Lee, “Detection of copy-rotate-move forgery using Zernike moments,” in Information Hiding. Berlin, Germany: Springer-Verlag, 2010, pp. 51–65.
[12] S. J. Ryu, M. Kirchner, M. J. Lee, and H. K. Lee, “Rotation invariant localization of duplicated image regions based on Zernike moments,” Aug. 2013.
[13] S. Bravo-Solorio , “Exposing duplicated regions affected by reflection, and scaling,” in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP), May 2011, pp. 1880–1883.
[14] H. Huang, W. Guo, and Y. Zhang, “Detection of copy–move forgery in digital images using SIFT algorithm,” in Proc. Pacific-Asia Workshop Comput. Intell. Ind. Appl. (PACIIA), Dec. 2008, pp. 272–276.
[15] X. Pan and S. Lyu, “Region duplication detection using image feature matching,” IEEE Trans. Inf. Forensics Security, vol. 5, no. 4, pp. 857–867, Dec. 2010.
[16] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, “A SIFT-based forensic method for copy–move attack detection and transformation recovery,” IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 1099–1110, Sep. 2011.
[17] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, “Image copy–move forgery detection based on SURF,” in Proc. Int. Conf. Multimedia Inf. Netw. Secur. (MINES), Nov. 2010, pp. 889–892.
[18] P. Kakar and N. Sudha, “Exposing postprocessed copy–paste forgeries through transform-invariant features,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, pp. 1018–1028, Jun. 2012.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 5, Special Issue 3, March 2016

6th International Conference in Magna on Emerging Engineering Trends 2016 [ICMEET 2016]

On 10th & 11th March, 2016

Organized by

Dept. of ECE, EEE & CSE, Magna College of Engineering, Chennai-600055, India.

[19] B. L. Shivakumar and S. S. Baboo, "Detection of region duplication forgery in digital images using SURF," IJCSI Int. J. Comput. Sci. Issues, vol. 8, issue 4. no. 1, pp. 199–205, 2011.
[20] D. G. Lowe, "Object recognition from local scale-invariant features," in Proc. 7th IEEE Int. Conf. Comput. Vis., Sep. 1999, pp. 1150–1157.
[21] H. Bay, T. Tuytelaars, and L. Van Gool, "SURF: Speeded up robust features," in Computer Vision. Berlin, Germany:
[22]C. T. Hsieh and Y. K. Wu, "Geometric Invariant Semi-fragile Image Watermarking Using Real Symmetric Matrix," WSEAS Transaction on Signal Processing, Vol. 2, Issue 5, May 2006, pp. 612-618.
[23] C. T. Hsieh, Y. K. Wu, and K. M. Hung, "An Adaptive Image Watermarking System Using Complementary Quantization," WSEAS Transaction on Information Science and Applications, Vol. 3, Issue 12, 2006, pp. 2392-2397.
[24] K. M. Hung, C. T. Hsieh and Y. K. Wu, "Multi-Purpose Watermarking Schemes for Color Halftone Image Based on Wavelet and Zernike Transform," WSEAS Transaction on Computer, Vol. 6, Issue 1, 2007, pp. 9-14.
[25] F. Hartung and M. Kutter, "Multimedia Watermarking Techniques," in Proceedings of the IEEE, Vol. 87, No. 7, July 1999, pp. 1079-1107