ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Image Forgery Detection Using Adaptive over Segmentation and Feature Point Matching

Manjushree Dr, Dr. Suresh L, Prof. Sandeep Kumar

M. Tech Student, Dept. of CSE, Cambridge Institute of Technology, Bangalore, India

Principal, Cambridge Institute of Technology, K R Puram, Bangalore, India

Associate professor, Dept. of CSE, Cambridge Institute of Technology, Bangalore, India

ABSTRACT: this work proposes for Image forgery detection using adaptive over segmentation and feature point matching. In forgery detection method proposes block based and key points integrates scheme, 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, and the forgery region extraction algorithm, which replaces the feature points with small super pixels as feature blocks and then merges the neigh boring blocks that have similar local color features into the feature blocks to generate the merged regions.

KEYWORDS: Copy-Move Forgery Detection, Adaptive Over-Segmentation, Local Color Feature, Forgery Region Extraction

I. INTRODUCTION

The world is getting advanced day by day as the technology is growing rapidly. According to the type of wish he needed, human develops different software's. Hence likewise now many image editing software are available. Using these tools the images get edited. This editing may have a positive face as well as a negative face. The negative face may cause for a human life itself. Now different editing tools are available that can edit the image in any way as they wish. Many morphological operations can be occurred in an image. These manipulations in an image are a serious issue regarding the authenticity, integrity, and reliability of the image.

More and more researchers have begun to focus on the problem of digital image tampering. Of the existing types of image tampering, a common manipulation of a digital image is copy-move forgery, which is to paste one or several copied region(s) of an image into other part(s) of the same image. 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 this case.

II. LITERATURE SURVEY

Amruta Jagtap et al [1] this paper Proposes a Verifying the integrity of images and detecting traces of tampering without requiring extra prior knowledge of the image content or any embedded watermarks is an important research field. An attempt is made to survey the recent developments in the field of digital image forgery detection. And a novel copy–move forgery detection scheme using adaptive over-segmentation and feature point matching. Also it explained the scheme integrates both block-based and key point-based forgery detection methods. 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

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

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.

A. J. Fridrich et al [2] described 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. This work comes under block-based forgery detection methods. 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. And 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.

Sreelakshmi M. et al [3] proposes for a Method Image features in an image can be added up or removed, without leaving any obvious traces in the image. Thus the method called forensic detection is used to detect such manipulations occurred in an image by recovering the history of an image. Here recovers the history of filtered JPEG image using an effective linear classifier that discriminates the forensic image with its trained data. Copy- move forgery is a type of image forgery where a portion of image gets copied and pasted at another location of the same image, which cannot be detected by naked eye. The method to detect such forgery is to initially segment the image using adaptive block segmentation and features are extracted from each image blocks and compare each blocks to one another to found out the match. Label the matched points to extract the forged region. Hence forged region is detected.

Musaed Alhussein et al [4] the image tampering includes both splicing and copy-move forgery. First, the image was decomposed into three color channels (one luminance and two Chroma), and each channel was divided into non-overlapping blocks. Local textures in the form of local binary pattern (LBP) were extracted from each block. The histograms of the patterns of all the blocks were concatenated to form a feature vector. The feature vector was then fed to an ELM for classification. The ELM is a powerful and fast classification approach. The experiment was performed using two publicly available databases. The experimental results showed that the proposed method achieved high detection accuracy in both the databases.

III. **PROPOSED SYSTEM**

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, it is 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 key point-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, 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.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

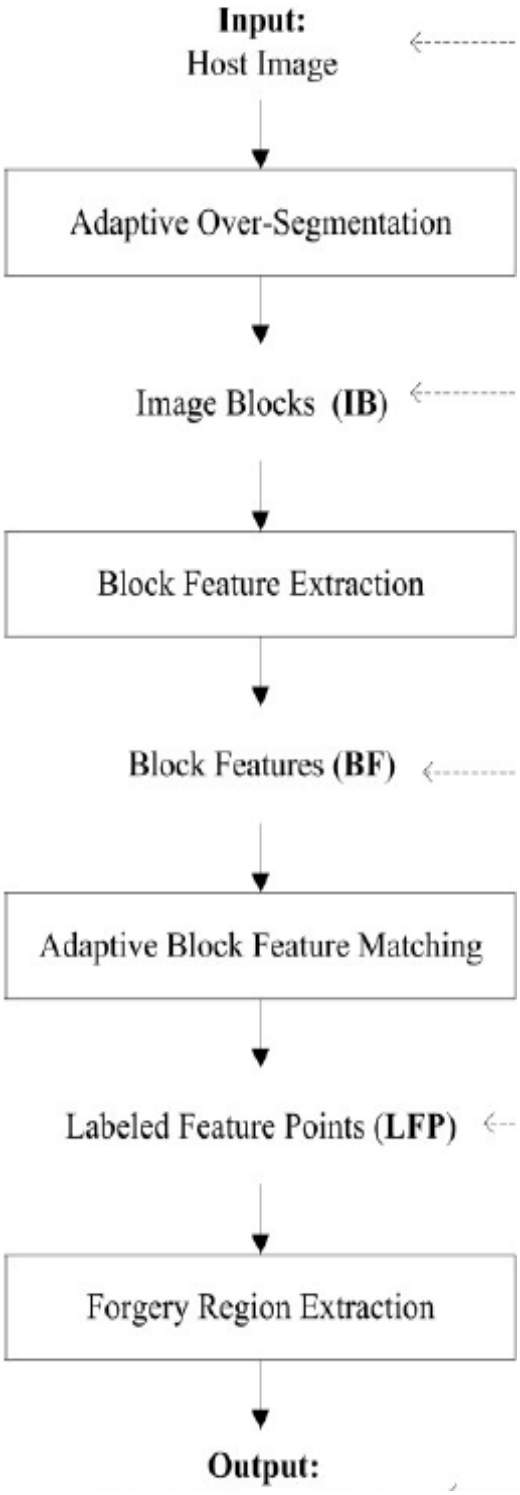


Figure 1: Framework of the Proposed Copy-Move Forgery Detection Scheme

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

a. Adaptive Over-Segmentation algorithm

The Adaptive Over-Segmentation algorithm, which is similar to when the size of the host images increases, the matching computation of the overlapping blocks will be much more expensive. To address these problems, we proposed the Adaptive Over-segmentation method, which can segment the host image into non-overlapping regions of irregular shape as image blocks afterward, the forgery regions can be detected by matching those non-overlapping and irregular regions. Segmentation method, the non-overlapping segmentation can decrease the computational expenses compared with the overlapping blocking; furthermore, in most cases, the irregular and meaningful regions can represent the forgery region better than the regular blocks. However, the initial size of the super pixels in SLIC is difficult to decide. In practical applications of copy-move forgery detection, the host images and the copy-move regions are of different sizes and have different content, and in our forgery detection method, different initial sizes of the super pixels can produce different forgery detection results; consequently, different host images should be blocked into super pixels of different initial sizes, which is highly related to the forgery detection results.

b. 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.

c. Block Feature Matching Algorithm

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 our algorithm, because the block feature is composed of a set of feature points, we proposed a different method to locate the matched blocks.

The detailed steps are explained as follows.

Algorithm: Block Feature matching algorithm

Input: Block Features (BF);

Output: Labeled Feature Points (LFP).

STEP-1: Load the Block Features BF ={BF1,BF2,... 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 BTR according to the distribution of correlation coefficients.

STEP-3: Locate the matched blocks MB according to the block matching threshold B TR.

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

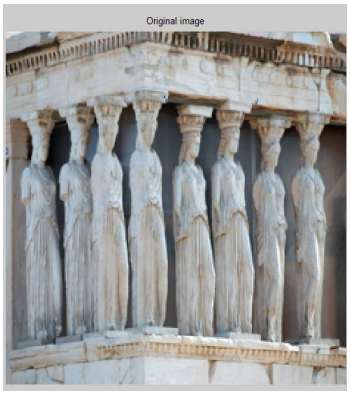
ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

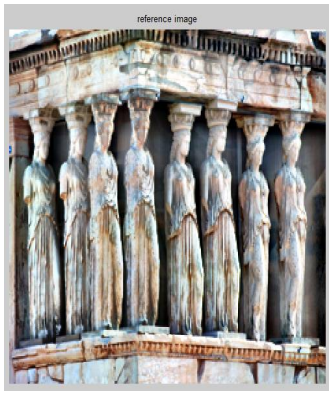
(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

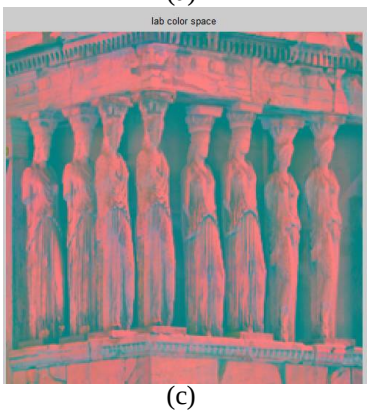
IV. RESULTS



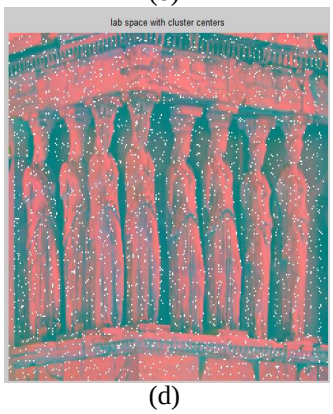
(a)



(b)



(c)



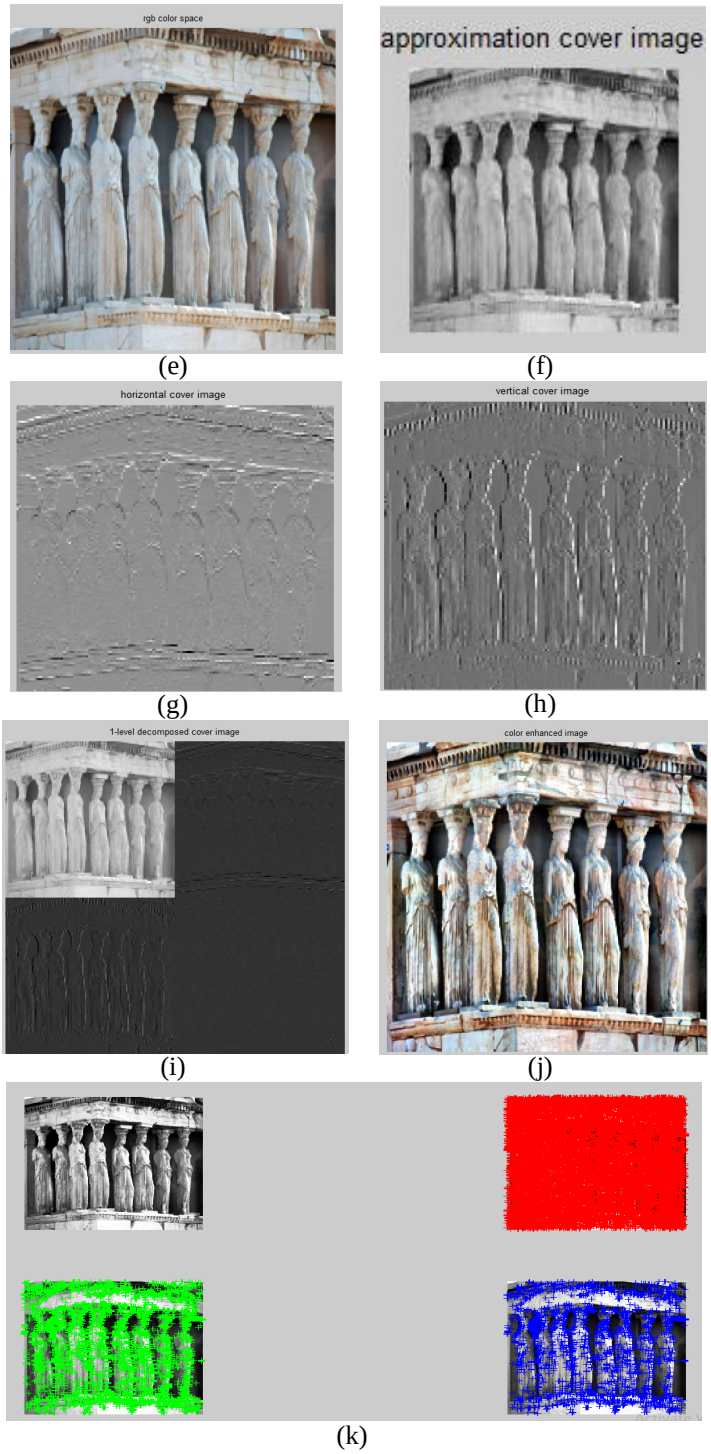
(d)

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016



(e) (f) (g) (h) (i) (j) (k)

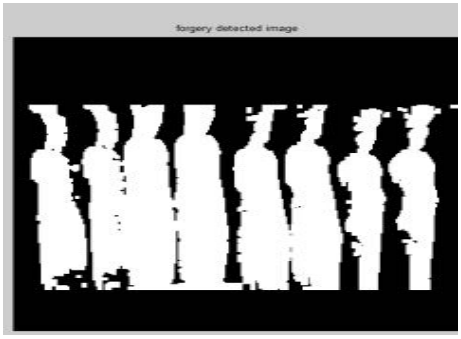
Figure 2: (a) Original Image; (b) Reference Image; (c) Lab Color Space; (d) Lab Space Cluster Centers; (e) Rgb Color Space; (f) Approximation Cover Image; (g) Horizontal Cover Image; (h) Vertical Cover Image; (i) 1-level decomposed cover image; (j) Color Enhanced Image; (k) Image Retrieval; (l) Forgery Detected Image:

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016



(l)

In this Proposed Results are Represents in Figure 2, will start with the Original image that is input image which is shows in figure (a), then take Reference Image shows in Figure (b), then it converting Color conversion based on RGB color conversion which is used image lab color image, and lab space cluster centers image shoes in figure (c, and, d) the approximate image are modified the Horizontal, vertical respective image, those are shows in figure (f, g, h)further modification are changing to the image enhance sing and 1-level decomposing image, and finally will got final result that is image retrieval shows in figure (k) and also Forgery Detected Image shows on figure (l)

V. CONCLUSION

This work concluded a 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. and The method to detect such forgery is to initially segment the image using adaptive block segmentation and features are extracted from each image blocks and compare each blocks to one another to found out the match. Label the matched points to extract the forged region. Hence forged region is detected.

REFERENCES

[1] Amruta Jagtap, H. A. Hingoliwala, H. A. Hingoliwala, “Survey Paper on Advanced Techniques for Image Forgery Detection”, International Journal of Science and Research (IJSR), Vol 4 Issue 12, 2015.
[2] A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, "Detection of copy-move forgery in digital images," 2003.
[3] Sreelakshmi. M, Amrutha M, “Forgery and Forensic Detection Using Adaptive over segmentation and DCT of JPEG Images”.
[4] Chi-Man Pun, Chen Yuan, Xiu-Li Bi,” Image Forgery Detection Using Adaptive Over-Segmentation and Feature Point Matching”.
[5] M.Meenakshi, K.S.Mohan,” A Novel Image Forgery Detection Approach By Using Scale Invariant Feature Transform”, International Research Journal of Engineering and Technology (IRJET), Vol 02, Issue 07, 2015.
[6] Shamna Parveen.S, Dr.D.Palanikkumar, “A Novel Approach For Inter Frame Copy Move Forgery Detection”, International Journal on Applications in Information and Communication Engineering, Vol 1, Issue 12, pp 60 – 62, 2015.
[7] Musaed Alhussein, “Image Tampering Detection Based on Local Texture Descriptor and Extreme Learning Machine”.
[8] Mr. Raskar Rahul Bhausaheb , Prof. Sandeep Kumar, Mr. Kharade Sachin, “Centroidal Distance Based Offline Signature Recognition Using Global and Local Features”, Vol 3, Issue 3, 2015.
[9] K.Girija, S.Herman Jeeva, M.Soniya, P.Sabarinathan, “Detecting Video Sequence Matching Using Segmentation Method”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 4, 2014.
[10] Svetlana Abramova, “Detecting Copy–Move Forgeries in Scanned Text Documents”.