A ROBUST APPROACH OF IMAGE FORGERY DETECTION AND LOCALIZATION

1 G. MADHUSUDhana RAO, 2 P. JAYA BABU, 3GADE KOUSAlya TEJASREE

1H.O.D & Associate Professor, Dept. of ECE, N.V.R College of Engineering & Technology, Tenali, A.P
2Assistant Professor, Dept. of ECE, N.V.R College of Engineering & Technology, Tenali, A.P
3M.Tech Scholar, Dept. of ECE, N.V.R College of Engineering & Technology, Tenali, A.P

ABSTRACT: This paper proposes for Image forgery detection using adaptive over segmentation and feature point matching. In forgery detection method block based and key points integrates scheme are proposed. Initially, the proposed adaptive over segmentation algorithm segments the host image into non-overlapping and irregular blocks adaptively. The feature points are extracted from each block as block features. The block features are compared with one another for locating the labeled feature points. This procedure can approximately specify the suspected forgery regions. To detect the forgery regions more accurately and efficiently, the forgery region extraction algorithm 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.

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

I. INTRODUCTION

Nowadays, digital image forgery has been becoming gradually easy to perform. The existing methods of image forgery, one of the common manipulations with digital image is copy-move forgery to paste one or several copied region(s) of an image into another part(s) of the same image. In the past years, many forgery detection methods have been proposed for copy-move forgery detection.

The existing methods can be divided in to two categories: the block-based forgery detection methods which are to segment the input images into overlapping and regular image blocks, and then obtain the forged regions by matching blocks of image pixels or their transform coefficients; and the key point-based forgery detection methods, which extract the image feature key points and match them to find the duplicated regions.

Although these methods are effective in forgery detection, they have three main drawbacks:
1) The input image is divided into overlapped regions, which will cause the computation complexity expensive;
2) The methods cannot deal with significant geometrical transformation of the forgery areas;
3) The host image is divided into regular blocks, which will cause low recall rate.

And the existing key point based forgery detection methods can somewhat reduce the computation complexity and can be strong against some attacks, the recall results were still poor. To address the shortcomings of the existing methods, we propose a novel copy-move forgery detection scheme using adaptive over-segmentation and feature point matching in this paper. The Adaptive Over-Segmentation algorithm is proposed to divide the host image into non-overlapping and irregular blocks. Then the feature points are extracted from each block and matched with each other to find the labelled feature points which can approximately specify the suspected forgery regions. Finally the labelled feature points are processed and the morphological operation is applied to generate the detected forgery regions.
II. RELATED WORK
With the help of powerful image editing software, we can easily modify digital images without leaving any perceptible artifacts. Maliciously tampered images would lead to some potentially serious consequences in our daily life. Therefore, image forensics has attracted considerable attention during the past decade. For most forensic methods, it is assumed that some inherent image statistics introduced by the generation pipeline will be inevitably distorted after some tampering operations, and researchers analyze such statistics so as to identify the forgeries. Generally, there are two main problems in image forensics, one is forgery detection, and the other one is forgery localization.

Forgery detection aims to discriminate whether a given image is pristine or fake. For instance, by exploiting some camera-related signals such as sensor pattern noise (SPN) and color filter array (CFA) properties, it is possible to reveal tampered images via camera source identification. By analyzing the JPEG compression artifacts, one can expose JPEG decompressed images and detect JPEG recompressed images. Based on the distinctive artifacts left by a certain operation, it can identify contrast enhancement reveal image re-sampling detect median filtering and so on. In practice, a key influential factor for forgery detection performance is the variety and uncertainty of tampering operations. Since most existing forensic methods assume that only one specific tampering operation is under investigation, they should not be used for a real forensic scenario independently. Usually, it requires to analyzing the image with several forensic detectors and combining the detection results using some fusion schemes.

Some recent works applied fuzzy theory and Dempster- Shafer theory to fuse the detection results, but these methods only considered JPEG compression artifacts, and might not be suitable for more general cases. An alternative solution is to seek for universal features that can identify as many tampering operations as possible.

In our previous work, we adopted some universal features in steganalysis to detect various image operations and identify their types. In a set of mixed moment features was proposed for the same topic. In order to evaluate the forensic performance in a practical situation, Information Forensics and Security Technical Committee (IFS-TC) established the First IFS-TC Image Forensics Challenge, whose first phase was forgery detection. In the challenge, advanced statistical features such as spatial rich model (SRM) were adopted by the winners. By simply merging the detection results of a statistical feature based detector and a copy move detector, meaning that the forensics community has achieved good performance for forgery detection.

II. PROPOSED METHOD
Visual evidences such as images provide a major clue, for resolving cases in the court of law and also images are the major information carriers in visual media. The today’s images are of digital form. The current digitization mechanisms have given the various significances of changing the properties and image quality. The existing image editing applications and software’s can improve the primary image content. Changing the image contents termed as image forging provides the viewer with false information as the changes made cannot be identified by the human eye.

This will have a serious effect where images are treated as proof for solving cases in the court of law. Also the modified digital images can be shared in social Medias, broadcasted in visual media and try to mislead the society. Hence there is requirement to verify the authenticity of
the image before considering it as an evidence for investigations in the court of law or publishing such false content images in visual broadcasting Medias and internet based social media. Digital Image forensics is an area which investigates the image contents to detect the forgeries imposed on the image. Digital image forensics deal with the study of different forgery attacks an image gets subjected to by a forger and the techniques to identify those attacks. The current image forgery techniques are more difficult to find. Many of the researches are being carried out to detect, localize it.

The recent studies focused on image forgery detection are capable of detecting the image tampering at higher accuracy through proper localization and mechanism specifications. But the detection tampered area of the image is still an open challenge i.e., localization issue. Thus, to overcome this many of the researchers have suggested for integration of different mechanisms for perfect localization. But, some of the challenges with images are still not studied properly i.e., of selection of forged area, fusing of different results. This paper is intended to provide efficient image forgery localization by using integration of statistical and copy move feature based methods.

The section describes the methodology used, where Figure (1) gives the proposed methodology block diagram. The first block represents the selection of forged image of interest which will be selected from the user defined folder. Later based on the features, the image is classified by extracting the features, LDA training, LDA based classification. In this, the copy move forgery is considered for detection which includes features extraction, matching of extracted features, and calculation of Mpm. Finally, the performance is evaluated by plotting the obtained ground truth values and parameter values like TP, TN, FP, FN, St, Sp, F1s and Pn are measured.

FIG 1: PROPOSED SYSTEM

The complete methodology is implemented over the MATLAB software system. The design implementation is described in this section which includes following algorithms.

A. Image Selection: This case of implementation gives the input image selection from the desired folder of user (UF). The user selects the name of the file (nF) and path of the file (pF). These nF and pF will direct to image path (Ipath). The input image (Ini) is chosen from the Ipath and is resized to get the original input image (Inimg).

B. Feature Based Classification: This contains three different stages like extraction of statistical features (EsF), training through Linear Discriminated analysis (LDA) (TLDA), classification based on LDA (CLDA). These stages are illustrated as below.

C. Extraction of Statistical Features: Before extracting the statistical features, the ground truth (GT) is considered. For GT, the image size (nr – rows and nc - columns) is taken into consideration, if the size is of 3 i.e.; RGB then converts it to Greyscale i.e., rgb2gray. Then obtained image is resized to get the GT image (GTimg).
For extraction, both the Inimg and GTimg are considered and then RGB color spaces (Cs) are obtained. The image is divided as block size of 3, from this center pixel (Cp) is obtained. The color image converted to Hue, Saturation, and Value (HSV) form. Then the empty features are initialized to get the statistical features (Sf). Later, calculated the features for every blocks and store in labels. Then obtained the vector for each color (Rv, Gv, Bv) and concatenate outcome to get vector (Cv). Finally, calculate the statistical features (Sf) by using Cv.

D. Linear Discriminated Analysis (LDA) Training: In this step of implementation for LDA training, the vectors formed during the Sf extraction i.e. F(ii)=(Sf)' and L(ii)=GTb. These F and L are initialized and its complements are represented with X and Y respectively. Finally, the LDA training is by using X and Y.

E. Feature Extraction: This part comes under the forgery detection where to extract the features following algorithm is implemented. The image size is considered. If image size is 3 i.e., colors (RGB) then convert it to greyscale. Then find the matrix form of image size and extract the scale invariant feature transform (SIFT) features. In this case of implementation original image and forged image sift features are stored in S1 and S2 respectively. In this case distance ratio is set to 0.6. Later matching is performed if matching found then collects matching features (Mf) at S3.

III. RESULTS
creating the image forgery on detection accuracy.

V. REFERENCES


