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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 7, Issue 3, March 2019

A Survey on Accurate and Efficient Image Forgery Detection Using SIFT Descriptor to Improve Detection Accuracy

Ashwini Vhanmane, Torana Kamble

ME Students, Department of Computer Science, BVCOE, Kharghar, Navi Mumbai, Mumbai University, India.

Professor, Department of Computer Science, BVCOE, Kharghar, Navi Mumbai, Mumbai University, India.

ABSTRACT: The developments of easy-to-use and advanced pictures editing software, the changes or copy paste of the contents of digital image has become very simple to do and it became hard to identify. A digital image is a very high or productive source of data and can capture any action correctly, that's why, its authenticity of the image or information is questionable. In the work, a novel passive picture forgery detection technique is introduced based on Image pre-processing techniques, Scale-Invariant Feature Transform (SIFT) descriptor for feature extraction to identify copy-move and splicing forgeries in input image. First, from the chrominance component of the input picture, particular localize features are extract by applying SIFT descriptor and using that features to identify the image is forgery or not and also using opencv technique to detect the forgery portion of target image.

KEYWORDS: Scale-Invariant Feature Transform (SIFT), Forgery Detection, Feature Extraction, copy-move forgery, splicing.

I. INTRODUCTION

In today's cyber world, the simple accessibility of profoundly progressed accessories and technology, and their large accessibility to every common man, has put the believability of digital data highly at stake. Today, neither a social security number, nor a credit card number, not even a bank account number can be used as an evidence, trustworthy enough to confirm one's identity. Digital images, being the major information carriers in today's digital world, act as the primary sources of evidence towards any event in the court of law as well as media and broadcast industries. Nonetheless, the relative simplicity of editing and manipulating digital images has made their validity and reliability largely questionable. In fact, seeing is no more believing, due to the fact that in today's digital age, there are an expanding number of vindictively altered pictures. Utilizing an extensive variety of effective software applications, digital image manipulations by an adversary have become extremely common and simple. One of the major issues in crime scene investigation depicted in an image is figuring out whether the image is genuine or doctored. This can be a critical assignment when images are utilized as fundamental proof to impact judgment, for instance, in the court of law.

Digital multimedia forensics has shown that statistical features intrinsic to images can be used to identify altered images. An important type of alteration to detect is the copy-paste image forgery, where image content is copied from one image and pasted into another, or same, image. This operation is often done to maliciously change the meaning or context of an image by inserting or concealing objects in it. Prior research has shown that copy-paste forgeries can be detected by finding localized inconsistencies in intrinsic image features such as traces of re-sampling, JPEG compression, contrast enhancement, median filtering and sensor noise. Additionally, techniques that work by finding duplicate image blocks and by matching SIFT features have been developed to detect copy-move image forgeries, where image content is pasted into the same image that it was cut from. Work in proposes a statistical framework for the fusion of such forgery detection features.

Two main categories of authentication methods in digital image forensics have been explored in literature: active methods and passive methods. Active methods embed digital authentication information (watermarks and extrinsic fingerprints) into the image content at the acquisition step. This information is retrieved during the authentication step

DOI: 10.15680/IJIRCCE.2019. 0703053

for comparison with the reference authentication data. These techniques are limited because authentication information can be embedded at the time of recording. Passive methods exploit image forgery without requiring explicit prior information. In addition, these methods expose image tampering by analyzing pixel-level correlations

Copy-move is a commonly used method for image forgery, in which one part of an image is copied and placed elsewhere in the same image. While pasting, the duplicated region may be post processed using rotation, scaling, blurring, or illumination changes.

II. RELATED WORK

In this work proposed to detect the image manipulation. Firstly the technique converts the input RGB image into YCbCr color channel that is chrominance component is divided into non-overlapping blocks. Second Local Binary Pattern (LBP) technique is performed, and wavelet transform technique is applied in all blocks. Finally Principle Component Analysis (PCA) technique is used for all blocks and the output is fed to Support vector Machine (SVM) classifier technique as features [1].

In this work, a novel passive image forgery detection method is proposed based on Local Binary Pattern (LBP) technique and Discrete Cosine Transform (DCT) technique to detect copy-move and splicing forgeries. First, from the chrominance component of the input image, discriminative localized features are extracted by applying 2D DCT technique in LBP space. Then, support vector machine (SVM) technique is utilized for detection [2].

This work presents a study of various picture forgery techniques and a survey of various attempts in copy-move forgery detection on images. A comparative analysis of major techniques is also presented in this work [3].

There are two types of image i.e. picture forgery detection copy move and picture splicing, and various attacks like blurring, noise, scaling, etc may occur. The overview of forgery detection technique, the basic flow of how the forged picture can be detected is presented. And lastly it is conclude with the comparative study with parameters, merits and demerits [4].

This study proposes a copy-move picture forgery detection technique using Hessian features and a center-symmetric local binary pattern (CSLBP)technique. The proposed method consists of four steps: (1) detecting the object based on normalized cut segmentation, (2) localizing the local interest points of each object based on the Hessian technique, (3) extracting CSLBP features, and (4) detecting duplicated regions in picture forgeries. Experiment results show that the method is robust to post processed copy-move forgery detection under scaling, and JPEG compression [5].

In this work, LBPs of DCT coefficients have been investigated for picture-splicing detection. Specifically, the LBP operator were used to model magnitude components of 2D arrays obtained by applying MBDCT to the test pictures; the resulting LBP technique features were served as discriminative features for picture-splicing detection. Owing to the high dimensionality of the proposed features, kernel PCA technique was therefore used for dimensionality reduction [6].

In this work, a Markov based approach in DCT technique and DWT technique domain is proposed for picture splicing detection. The proposed feature vector contain of two kinds of Markov features generated from the transition probability matrices; say the expanded Markov features in DCT domain and the Markov features in DWT domain [7].

This work describes blind forensics approach for detecting Copy-Move forgery on image. Our technique works by first applying DWT (Discrete Wavelet Transform) technique to the input picture to yield a reduced dimension representation. Then the compressed picture is divided into overlapping blocks. These blocks are then sorted and duplicated blocks are identified using Phase Correlation as similarity criterion. Due to DWT technique usage, detection is first carried out on lowest level picture representation [8].

In this work, propose a passive copy move picture forgery detection method using a steerable pyramid transform (SPT) technique and Local Binary Pattern (LBP) technique. SPT technique is applied on a grayscale version or one of the YCbCr channels of a picture. LBP technique is applied to describe the texture in each SPT technique sub band. Then the support vector machine (SVM) technique uses the LBP technique feature extracted from SPT technique sub-bands in classifying pictures into tampered or authentic pictures [9].

In this work, they have adopted key point-based features for copy–move picture forgery detection on images; however, our emphasis is on accurate and robust localization of duplicated regions. In this context, they are interested in estimating the transformation (e.g., affine) between the copied and pasted regions of picture more accurately as well as extracting these regions as robustly by reducing the number of false positives and negatives. To address these issues, we propose using a more powerful set of key point based features, called MIFT, which shares the properties of SIFT technique features but also are invariant to mirror reflection transformations [10].

Problem statement

The technique of creating duplicate picture has been extremely easy with the introduction of new and powerful computer graphic editing software which are free of cost available as Photoshop, GIMP, and Corel Paint Shop. Today, this powerful picture processing software's allowed people to change pictures and pictures conveniently and invisible. Now-days it creates a big challenge to authenticate the pictures. So our proposed system will work on this issue to produce a new application to identify and detect the forgery part on specific picture.

Purpose Scope

Sometimes it is difficult to identify the edited region from the original picture. The identification of a forged picture is driven by the need of authenticity and to keep up integrity of the unique picture.

Objectives

- To implement image preprocessing techniques
- To implement image feature extraction techniques
- To identify the image is forged or not.
- To detect forged image regions
- To reduce the time for detection and identification of forgery using opencv

III. PROPOSED SYSTEM

In this work, we will proposed a image forgery detection application introduced based on Image pre-processing techniques, Scale-Invariant Feature Transform (SIFT) descriptor for feature extraction to identify copy-move forgeries in input image. First, from the chrominance component of the input image are extracted i.e. image will be converted into YCbCr format, after that particular localize features are extract by applying SIFT descriptor and using that features will identify the image is forgery or not. Also using opencv technique will detect the forgery portion of target image.

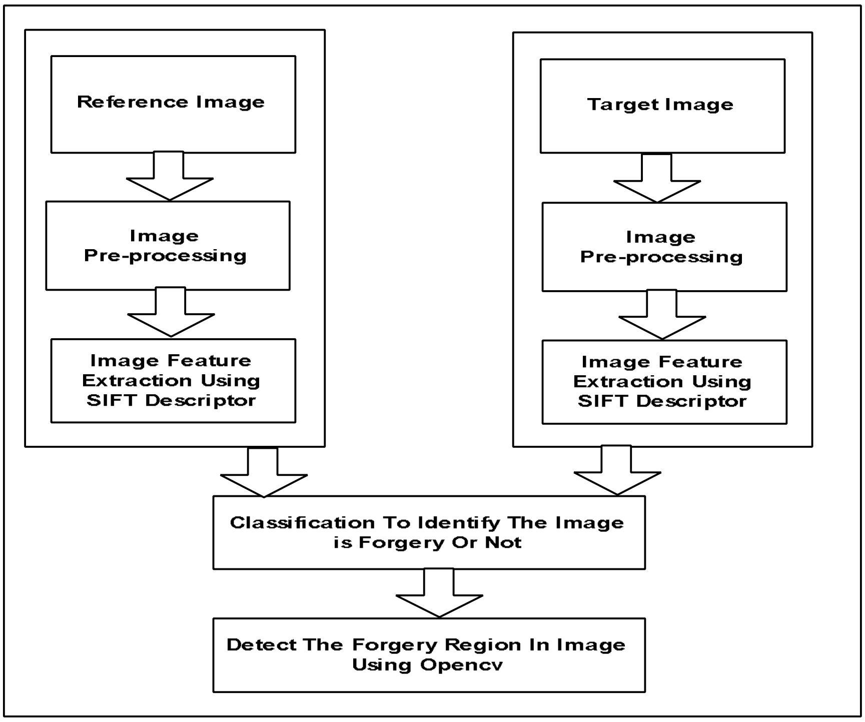
Reference Image
Image Pre-processing
Image Feature Extraction Using SIFT Descriptor
Target Image
Image Pre-processing
Image Feature Extraction Using SIFT Descriptor
Classification To Identify The Image is Forgery Or Not
Detect The Forgery Region In Image Using Opencv

Fig 1: Proposed System Architecture

Project Workflow Diagram:

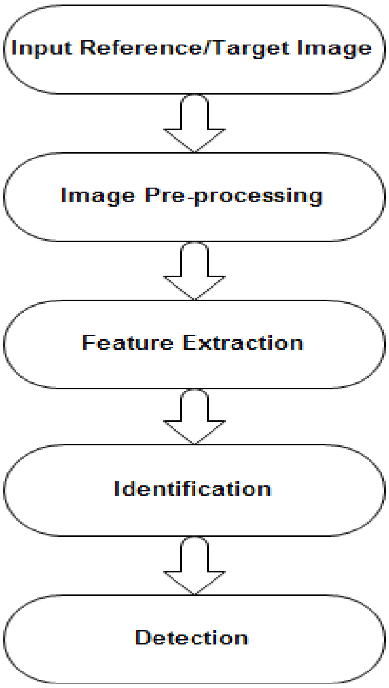

Fig 2: Proposed Workflow

IV. ALGORITHM

Scale Invariant Feature Transform (SIFT)

A SIFT key point is a image region with an orientation. It is described by a geometric frame of four parameters: the key point center coordinates x and y, its scale (the radius of the region), and its orientation (an angle expressed in radians). The SIFT detector uses as key points image structures which resemble “blobs”. By searching for blobs at multiple scales and positions, the SIFT detector is invariant (or, more accurately, covariant) to translation, rotations, and are scaling of the image.

The key point orientation is also determined from the local image appearance and is covariant to image rotations. Depending on the symmetry of the key point appearance, determining the orientation can be ambiguous. In this case, the SIFT detectors returns a list of up to four possible orientations, constructing up to four frames (differing only by their orientation) for each detected image blob.

Steps:

1. Initialize a SIFT filter object with **vl_sift_new ()**. The filter can be reused for multiple images of the same size (e.g. for an entire video sequence).
2. For each octave in the scale space:
    a. Compute the next octave of the DOG scale space using either **vl_sift_process_first_octave()** or **vl_sift_process_next_octave()** (stop processing if **VL_ERR_EOF** is returned).
    b. Run the SIFT detector with **vl_sift_detect ()** to get the key points.
    c. For each key point:
        i. Use **vl_sift_calc_keypoint_orientations ()** to get the key point orientation(s).
        ii. For each orientation:
            1. Use **vl_sift_calc_keypoint_descriptor ()** to get the key point descriptor.

3. Delete the SIFT filter by **vl_sift_delete ()**.
4. To compute SIFT descriptors of custom key points, use **vl_sift_calc_raw_descriptor ()**.

V. CONCLUSION

This work presents the image forgery detection based on Scale Invariant Feature Transform (SIFT) which finally all extracted features will give the final result. In this work we presented a novel technique for unsupervised forensic analysis of image file containers. To achieve the forgery detection in the image file content, defined by different manufacturers, models and software processing. Will proposed the first formal approach to perform integrity verification and difference identification and classification based on such features. Our outcome will demonstrates that the proposed strategy will be very effective in detecting image forgery and its accuracy will be acceptable compared to the other techniques

REFERENCES

[1] Fahimehakimi, Mahdi Hariri, farhadGharehBaghi, “Image Splicing Forgery Detection using Local binary pattern and Discrete Wavelet transform”, 2015 2nd International Conference on Knowledge-Based Engineering and Innovation.

[2] AmaniAlahmadi, Muhammad Hussain, HatimAboalsamh, GhulamMuhamma, George Bebis, Hassan Mathkour, “Passive Detection of Image Forgery using DCT and Local Binary Pattern”

[3] Rani Susan Oommen, Jayamohan M., Sruthy S., “A Survey of Copy-Move Forgery Detection Techniques for Digital Images”, International Journal of Innovations in Engineering and technology.

[4] CharmilNitinBharti, PurviTandel, “A Survey of Image Forgery Detection Techniques”, IEEE WiSPNET 2016 conference

[5] Diaa M. Uliyan, Hamid A. Jalab, Ainuddin W. Abdul Wahab, “Copy Move Image Forgery Detection Using Hessian and Center Symmetric Local Binary Pattern”, 2015 IEEE Conference on Open Systems (ICOS), August 24-26, 2015, Melaka, Malaysia

[6] Yujin Zhang, Chenglin Zhao, Yiming Pi, Shenghong Li, and Shilin Wang, “Image-splicing forgery detection based on local binary patterns of DCT coefficients”

[7] He, Z., W. Lu, Digital image splicing detection based on Markov features in DCT and DWT domain, Pattern Recognition 45(12), 4292-4299 (2012)

[8] Khan S and Kulkarni A. An efficient method for detection of copy move forgery using discrete wavelet transforms. International Journal on Computer Science and Engineering 2010, 2(5): 1801-1806

[9] G. Muammad, M.H. Al-Hammadi, M. Hussain, A. M. Mirza, and G. Bebis,” Copy Move Image Forgery Detection Method Using Steerable Pyramid Transform and Texture Descriptor” in Proc. EUROCON 2013. Image Processing and Analysis.

[10] Jaberi, M., Bebis, G., Hussain, M., Muhammad, G., Accurate and robust localization of duplicated region in copy-move image forgery, Machine Vision and Applications, 25(2), 451-475 (2014).