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 5, May 2019

Accurate and Efficient Image Forgery Detection Using Local Binary Pattern Technique

Avinash Dahibhate, Sumit Chaudhari, Nikita Marathe, Ankita Narsale, Prof. V. M. Lomte

B. E Students, Department of Computer Engineering, RMDSSOE Pune, India

Professor, Department of Computer Engineering, RMDSSOE Pune, 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 become hard to identify. A digital image is a very high or productive source of data and can catching 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, Local Binary Pattern (LBP) 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 LBP space and using that features to identify the image is forgery or not and also using opencv technique to detect the forgeries of target image.

KEYWORDS: Local Binary Pattern (LBP),Forgery Detection, Feature Extraction, copy-move forgery, image splicing.

I. INTRODUCTION

Digital multimedia forensics has shown that statistical features intrinsic to images can be used to identify altered or forgedimages. An important type of alteration to detect is thecopy-paste image forgery, where image content is copied fromone image and pasted into another or same image. Thisoperation is often done to maliciously change the meaningor context of an image by inserting or concealing objects init. Prior research has shown that copy-paste forgeries can bedetected by finding localized inconsistencies in intrinsic imagefeatures such as traces of re-sampling, JPEG compression, contrast enhancement, median filtering and sensor noise. Additionally, techniques that workby finding duplicate image blocks and by matchingSIFT features have been developed to detect copy-moveimage forgeries, where image content is pasted into thesame image that it was cut from. Work in proposes astatistical framework for the fusion of such forgery detectionfeatures.

Two main categories ofauthentication methods in digital image forensics have beenexplored in literature: active methods and passive methods. Active methods embed digital authentication information(watermarks and extrinsic fingerprints) into the image content atthe acquisition step. This information is retrieved during theauthentication step for comparison with the referenceauthentication data. These techniques are limited becauseauthentication information can be embedded at the time ofrecording. Passive methods exploit image forgery withoutrequiring explicit prior information. In addition, these methodsexpose image tampering by analyzing pixel-level correlations
Copy-move is a commonly used method for image forgery, inwhich one part of an image is copied and placed elsewhere inthe same image. While pasting, the duplicated region may bepostprocessed using rotation, scaling, blurring, or illuminationchanges.

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 techniqueas features [1].

In this work, a novel passive image forgery detection method is proposed based on Local Binary Pattern (LBP) techniqueand Discrete Cosine Transform (DCT) techniqueto 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 presentedin 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 techniqueusing 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 techniquewas therefore used for dimensionality reduction [6].

In this work, a Markov based approach in DCT techniqueand DWT techniquedomain 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 techniqueis applied on a grayscale version or one of the YCbCr channels of a picture. LBP techniqueis applied to describe the texture in each SPT techniquesub band. Then the support vector machine (SVM) techniqueuses the LBP techniquefeature extracted from SPT techniquesub-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 [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.

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, Local Binary Patternfor 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 LBP and using that features will identify the image is forgery or not. Also using opencv technique will detect the forgery portion of target image.

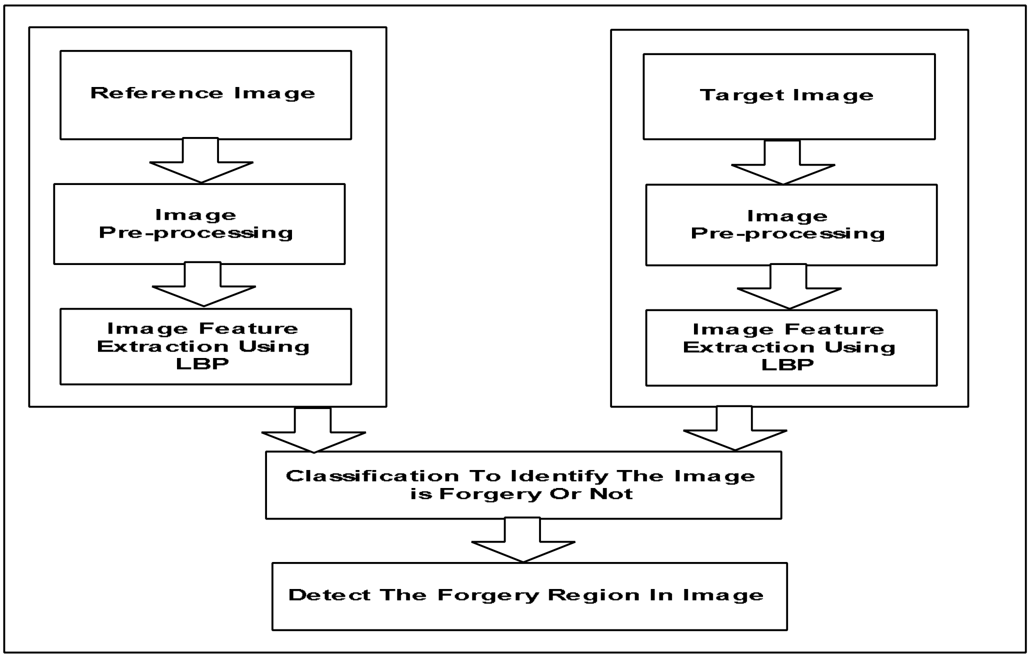
Reference Image
Image Pre-processing
Image Feature Extraction Using LBP
Target Image
Image Pre-processing
Image Feature Extraction Using LBP
Classification To Identify The Image is Forgery Or Not
Detect The Forgery Region In Image

Fig 1: Proposed System Architecture

Project Workflow Diagram:

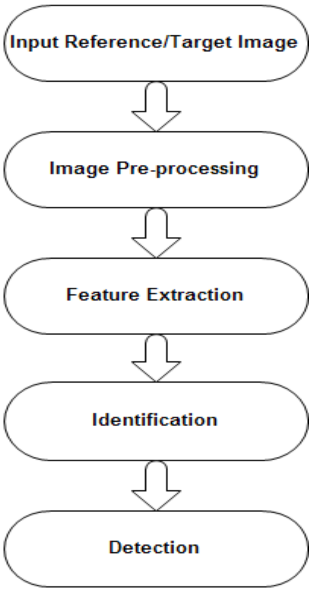

Fig 2: Workflow Diagram

IV. ALGORITHM

LBP for Feature Extraction:

LBP is a texture descriptor that labels each pixel in the image by thresholding the neighborhood pixels with the center pixel and considering the result as a binary number.
Then, the texture can be described by the histogram of these label values. A basic LBP operator is calculated in a rectangular window. LBP can also be extracted in a circular neighborhood (P, R), where P is the number of neighbors and R is the radius of the neighborhood. In this work, we have experimented both with the basic and circular LBP using P = 8 and R = 1. The results are reported with circular LBP only. The normalized LBP histogram is used as a feature vector for the corresponding block. The histogram has 256 bins corresponding to 256 gray values. The reason behind using LBP is that we are interested in texture, which remains similar in the copied and pasted area even some post-processing is applied after forgery. Therefore, the texture pattern can be a good indicator of forgery detection

The descriptors $f_i$for each segment S_i is calculated, whichcombines the strength of Hessian features and ofLBP texture analysis. The LBP can be defined as a modified version of the local binary pattern (LBP).
Mathematically, the LBP is defined as,

$$\mathrm{LBP}\ (x_c\ ,y_c\ ) = \sum_{n=0}^{n=7} s(g_n\ -\ g_c)\ 2^n$$

$$\mathrm{S(x)} = \begin{cases} 1, x\ \geq 0 \\ 0.\ otherwise \end{cases}$$

Where$g_c$is the gray value of the center pixel (x_c,y_c), and $g_n$represents eight neighboring pixels. If $g_n$is smaller than g_c, thenthe binary result of the pixel is set to 0; otherwise, it is set to 1.In LBP, instead of comparing the neighboring pixels with thecenter pixel, the center-symmetric pairs of pixels, such as (*g0*,*g4*), (*g1*, *g5*), (*g2*, *g6*), and (*g3*, *g7*), are computed as follows

$$\text{LBP}(x_c, y_c) = \sum_{n=0}^{n=3} s(g_n - g_{n+4})\, 2^n$$

$$S(x) = \begin{cases} 1, x \geq 0 \\ 0. otherwise \end{cases}$$

V. RESULT

Graph 1:

Table 1, 2 represents detection accuracy when large size and small size of forgery present in image is analyzed. Images with large size forgery shows highest accuracy and less number of false positives among all three cases of different forgery size image. Table shows comparative results for copy-move forgery detection. Proposed method can accurately detect forged areas.

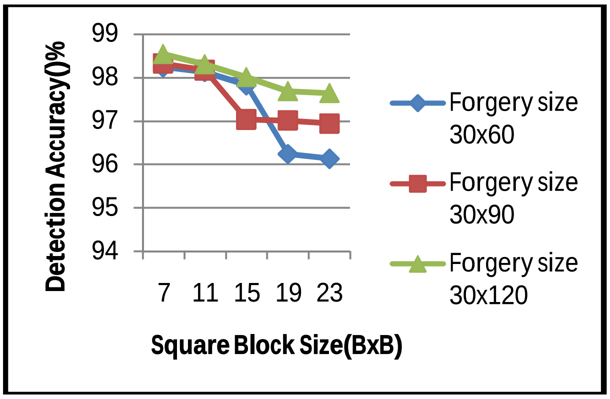

Fig.3. Detection Accuracy for small image forgery detection

Result Table1:

	Forgery size 30x60	**Forgery size 30x90**	**Forgery size 30x120**
7	98.2388	98.3217	98.5467
11	98.1255	98.17	98.3106
15	97.8237	97.039	98.018
19	96.2465	97.012	97.693
23	96.1372	96.9456	97.6456

DOI: 10.15680/IJIRCCE.2019. 0705021

Graph 2:

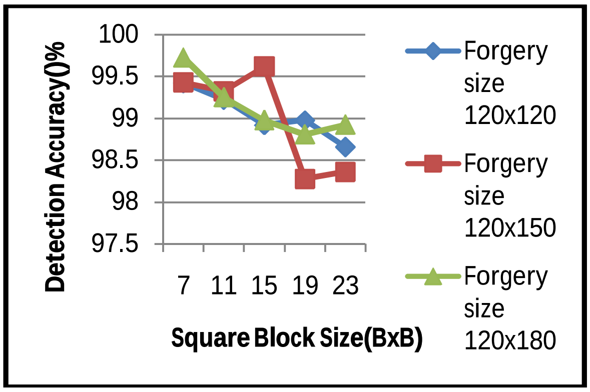

Fig.4. Detection Accuracy for large size image forgery detection

Result Table2:

	Forgery size 120x120	Forgery size 120x150	Forgery size 120x180
7	99.4236	99.429	99.7238
11	99.2245	99.3245	99.2495
15	98.9189	99.6189	98.9768
19	98.9756	98.2755	98.8067
23	98.6574	98.3584	98.9236

VI. CONCLUSION

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. Proposed work will use LBP technique for image feature extraction to identify the image is forgery or not.Will proposed the first formal approach to perform integrity verification and difference identification and classification based on such features.

REFERENCES

[1] Fahime hakimi, Mahdi Hariri, farhad GharehBaghi, “Image Splicing Forgery Detection using Local binary pattern and Discrete Wavelet transform”, 2015 2nd International Conference on Knowledge-Based Engineering and Innovation.
[2] Amani Alahmadi, Muhammad Hussain, Hatim Aboalsamh, Ghulam Muhamma, 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] Charmil Nitin Bharti, Purvi Tandel, “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).