IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 4, Ver. I (July – Aug. 2015), PP 66-70
www.iosrjournals.org

Copy-Move Image Forgery Detection Based on Center-Symmetric Local Binary Pattern

[1]Vandana Sangwan, [2]Madan Lal
[1, 2] Department of Computer Engineering Punjabi University Patiala-147002, (India)

Abstract: *This paper presents a method to detect copy-move image forgery using CS-LBP (centre symmetric local binary pattern), an extension of basic local binary pattern. In the proposed method, firstly gray level conversion is performed on the given image. Later, the image will be decomposed into fixed sized non-overlapping blocks. Feature extraction can be done using CS- LBP, as this technique is invariant to illumination and rotation. Then distance between the extracted feature vectors is calculated and are sorted lexicographically, and retained only those pairs of blocks that have minimal distances between them. Those minimal distances compared with predefined threshold value serve as the purpose of the copied regions. In the end, post-processing is done using morphological operation and mask is generated for the region detected as forged region.*

Keywords: *Copy-move forgery detection, CS-LBP, feature extraction, Image Tampering.*

I. Introduction

In today's technological era, digital images are the basic form of conveying information. But the authenticity of these images is a big question for the society. As digital images are used in every field, for example medical imaging, satellite imaging, forensic labs, and journalism for easy visualization, so preserving their originality is a major issue. The popularity of digital images leads to the research in this area. With the help of easy availability of photo editing software, an image can be tampered easily. This image tampering is basically image forgery which is carried out to present false information or modify the real content of the image.

There are three main classes of image forgery, namely image retouching, copy-move forgery and image splicing. Image re-touching involves rotation, scaling, contrast enhancement and resizing. In copy-move forgery, an object or portion of the image is copied and pasted on to the other location in the same image so as to hide some information or alter the original content of the image. Here, the basic characteristics of the image remain same such as color, texture. Thirdly, the image splicing is a forgery that is a combination of two or more than two images and results into a new image. Image splicing sources are heterogeneous as contents can be picked from anywhere. The approaches to detect the digital image forgery are classified into two categories, active and passive. In active forgery, some form of watermarking information is present in the image. In passive or blind forgery, there is no such information is hidden in the image. Copy move forgery is an example of passive (blind) forgery which will be detected using center-symmetric local binary pattern scheme.

In this paper, a passive method to detect copy move forgery in digital images is proposed. Firstly, we divide the image into overlapping blocks after converting it into gray scale. Then using CS-LBP, feature vectors are to be extracted. This technique overcomes with the drawbacks of basic local binary pattern, such as variant to illumination and it is not too robust on flat image areas i.e. variance of intensity values within the uniform region is very low. CS-LBP preserves better gradient information while preserving distinctiveness, reduce dimensions also. Then lexicographical sorting is done on the feature vectors so as to bring the similar pairs of vectors together for easy recognition. Finally the distance between those vectors is calculated and compared with a threshold value to detect the duplicated region. The rest of the paper is as follows. In section 2, some previously related work has being discussed, section 3 introduces CS-LBP operation. In section 4, proposed algorithm is presented, followed with the results and conclusion in section 6.

II. Related Works

In this section, we have reviewed the passive methods for detection of copy-move forgery. Among the initial attempts J. Fridrich, D. Soukal and J. Lukas [1] proposed methods to detect copy-move forgery. Discrete cosine transform (DCT) of the image blocks was used and their lexicographical sorting is taken to avoid the computational burden. Once sorted the adjacent identical pair of blocks are considered to be copy-moved blocks. Block matching algorithm was used for balance between performance and complexity. This method suffers from the drawback that it cannot detect small duplicate regions. Mohammad Farukh Hashmi, Vijay Anand, Avinas G Keskar [2] proposed method using un-decimated wavelet transform along with SIFT operator to extract more number of key-points that are matched to detect the copied blocks efficiently. This method gives better results than DWT.

Mohammad Hussain et al, [3] showed a method based upon multi-resolution Weber law descriptors (WLD. The suggested multi-resolution WLD extracts the features from chrominance components. An SVM is used for classification and the experimental results showed that the accuracy rate can reach up to 91%.

Ning Zheng, Yixing Wang and Ming Xu [4] used a block based method to describe the components extracted using LBP operator which is rotationally invariant. This method gives better results to post-processing and rotation effects. Later on, technique presented by B.L. Shiva kumar et al, [5] using SURF and KD-tree for data matching step results in minimal false matches if images of high resolution being taken.

Reza Davarzani, Khashayar Yaghmie et al, [6] presented a method based on multi-resolution local binary pattern. This method is robust to geometric changes and illumination variations of the copied portions. They proposed this method against after various variations such as rotation, blurring, noise addition, and JPEG compression.

Motasem Alsawadi et al, [7] introduced a method based on basic local binary pattern with neighborhood clustering to refine the features. This method shows the reduction in matching false regions.

Various techniques have been proposed and research is still going on. We tried to put our novel method using variation of LBP, which is CS-LBP, so as to overcome the problems faced with local binary pattern.

III. Proposed Algorithm

The proposed step-wise methodology is as shown in fig.1.

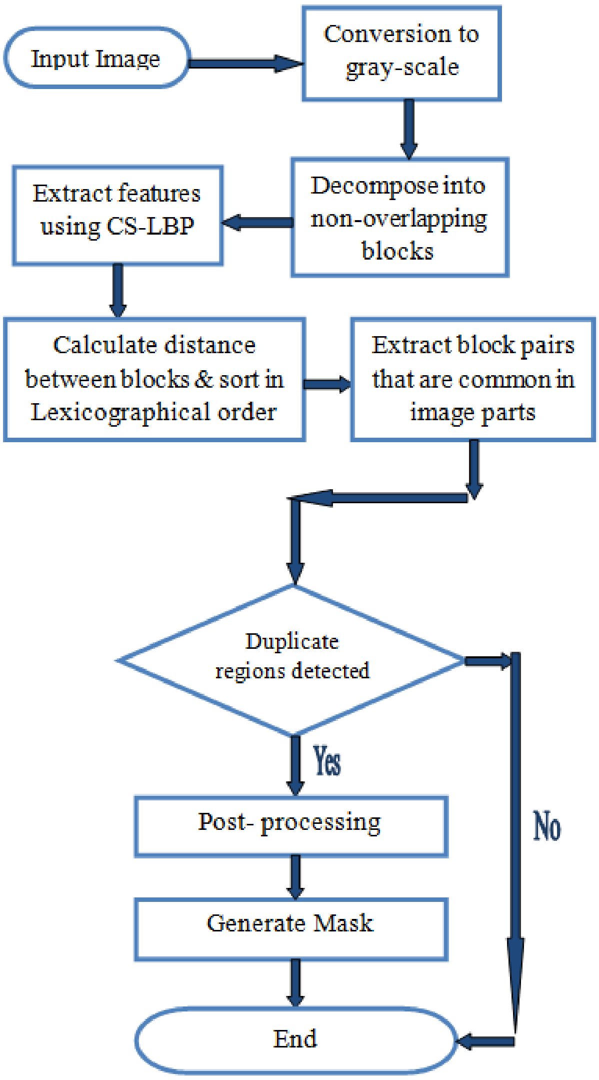

Fig. 1 Block diagram of proposed method

Step-1: Gray Scale Conversion
Firstly, the given input image is converted to gray scale according to the following equation.

$$Y = 0.299R + 0.587G + 0.114B \quad (1)$$

Where, Y is luminance component. Also a gray scale image is simple to work with.

Step-2: Division of image into overlapping blocks
The next step is to decompose the image (gray scale image) into fixed sized overlapping blocks. The block size is chosen to be the minimal size of image tampering portion. For an image of size M*N, the total number of blocks formed are given as per the following equation.

$$TB = (M-B+1)(N-B+1) \quad (2)$$

Step-3: Feature extraction using CS-LBP
In this phase, features are extracted from the blocks using center-symmetric local binary pattern. CS-LBP is a variant of local binary pattern, which is free from illumination variances and rotation effects. CS-LBP also yields less number of feature vectors as compared to LBP so to make this technique less time consuming, as shown in fig.2. For an image of M*N dimensions, local binary pattern produces 256 different binary patterns, whereas for CS-LBP this number is only 16. Furthermore, robustness on flat image regions is obtained by thresholding the gray-level differences with a small value T.

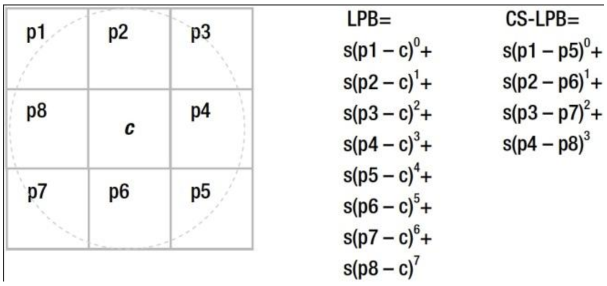

Fig. 2 Extraction of CS-LBP feature vectors The value of the threshold T is 1% of the pixel value

$$\mathrm{CSLBP}_{R,N,T}(x,y) = \sum_{i=0}^{(N/2)-1} s\left(n_i - n_{i+(N/2)}\right) 2^i,$$

$$\text{Where } s(x) = \begin{cases} 1 & x > T \\ 0 & \text{otherwise} \end{cases} \quad (3)$$

Range in our experiments. Since the region data lies between 0 and 1, T is set to 0.01. The radius is set to 2 and the size of the neighborhood is 8. It should be noted that the gain of CS-LBP over LBP is not only due to the dimensionality reduction, but also to the fact that the CS-LBP captures better the gradient information than the basic LBP.

A texture descriptor used in passive forgery detection of copy move forgery should be rotationally invariant, so that if the copied region is rotated before pasting into the same image, it can still be detected. Rotational invariant CSLBP can be express by the Eq. (2):

$\mathrm{CSLBP}^{ri}_{N,R} = \min\{ROR(\mathrm{CSLBP}_{N,R}, i) \mid i==0,1\ldots N\}$ Eq. (2)

Where, function ROR (z, i) represents circular bitwise rotation of sequence z by i steps.

Step-4: Calculation of distance & Lexicographical sorting

$dij = \sqrt{(xi - xj)^2 + (yi - yj)^2}$ where (x_i, y_i) is the top-left corner's coordinate of the i-th block.

This type of sorting is applied on the rows of the matrix. In the organized list, homogeneous rows are proximate to each other.

Step-5: Post-Processing
Morphologic operations are applied to fill the holes in the marked regions and remove the isolated points, then output the final result.

IV. Results

The experiments were carried on Dell laptop having Core2 Duo processor with 2GB RAM using MATLAB 2012a.The database on which we conducted our test contains a total of 220 images, in which 110 images are original images and remaining 110 images are forged images.

Also, true positive rate and false positive rate is being calculated to analyze the performance of the proposed system quantitatively. TPR is the percentage of correctly identified forged images while FPR is the percentage of original images falsely identified as forged.

$$TPR(\%) = \frac{\begin{array}{c} no.of\ forged\ images \\ detected\ as\ forged \end{array}}{total\ no.of\ forged\ images} \times 100$$

$$FPR(\%) = \frac{\begin{array}{c} no.of\ original\ images \\ detected\ as\ forged \end{array}}{total\ no.of\ original\ images} \times 100$$

Fig. 3: (a) Original image, (b) CS-LBP extracted feature representation,(c) forged image,(d) shows the generation of mask of forged area in the image.

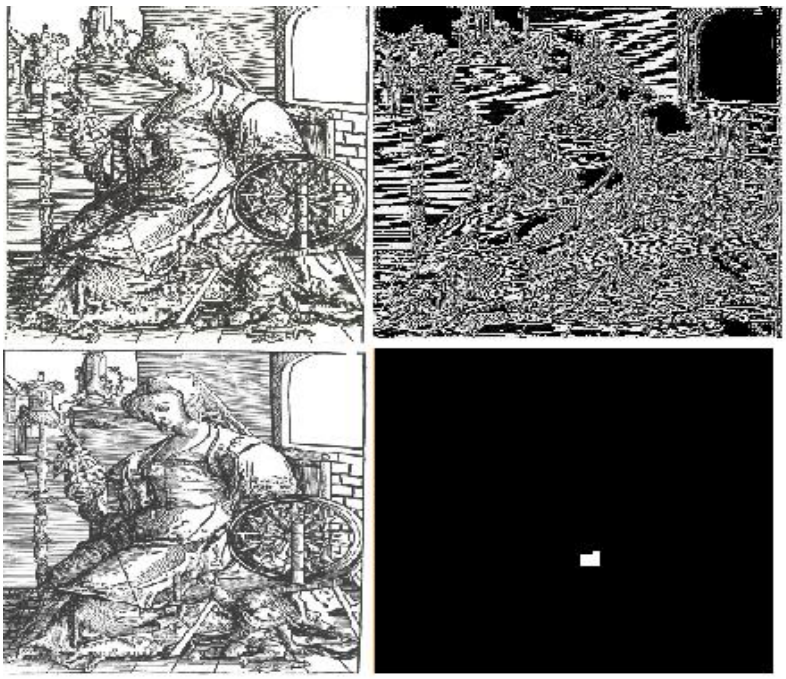

Fig. 4: (a) Original image, (b) Feature extraction using CS-LBP, (c) forged image, (d) shows mask generation of the forged portion in image.

V. Conclusion

A novel CS-LBP interest region descriptor which combines the strengths of the well known SIFT descriptor and the LBP texture operator was proposed. SIFT operator reduces the length of feature vector, so analyzing feature vectors will take less time. This method gives better result than using LBP alone, TPR ratio value is more, while the false positives are decreased using morphological operation. Overall accuracy of the proposed system outperforms simple LBP technique. There can be a scope for future work on this technique such as verifying this technique on other image formats and also different post-processing effects.

References

[1]. J. Fridrich, B. D. Soukal, and A. J. Lukas, "Detection of copy move forgery in digital images," in Proceedings of the Digital Forensic Research Workshop, Cleveland, Ohio, USA,August 2003.

[2]. Mohammad Farukh Hashmia et al, "Copy-move Image Forgery Detection Using an Efficient and Robust Method Combining Un-decimated Wavelet Transform and Scale Invariant Feature Transform" 2014 AASRI Conference on Circuit and Signal Processing (CSP 2014).

[3]. G. Muhammad, M. Hussain, G. Bebis, "Passive copy move image forgery detection using undecimated dyadic wavelet transform," Digital Investigation, vol. 9 (1), pp. 49-57, 2012.

[4]. Ning Zheng, Yixing Wang and Ming Xu, "A LBP Based Method for Detecting Copy-Move Forgery with Rotation," Springer Science, pp. 261-267,2013.

[5]. B. L. Shivakumar and Lt. Dr. Santhosh. "Detecting copy-move forgery in Digital images: A survey and analysis of current methods," Global Journal of Computer Science and Technology, vol. 10, no. 7, 2010.

[6]. R. Davarzani, K. Yaghmaie, S. Mozaffari, and M. Tapak, "Copymove forgery detection using multiresolution local binary patterns", Forensics Science International, vol. 231, pp. 61-72, 2013.

[7]. Motasem Alsawadi et al, "Copy-Move Image Forgery Detection Using Local Binary Pattern and Neighborhood Clustering," IEEE, pp. 249-254, 2013.