Volume 6, Issue 1, January 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Fast Copy-Move Forgery Detection Scheme Using Patch - Based Descriptors

Rameeza M Ashraf
M.Tech Student, KMEA
CSE Department, M.G. University,
Kerala, India

Veena K Viswam
Assistant Professor, KMEA
CSE Department, M.G. University,
Kerala, India

Abstract— Forgery is the process of creating, flexible, or emulating documents with the aim of altering the details or to earn profit from the forged item. Nowadays, digital images are a popular source of information. With the advancements in powerful computer graphics the process of creating fake images is very simple. Tampering of these digital images is known as Image Forgery. A common forgery approach is the copy move .Copy move forgery is the process of creating a forged item by copying a region of the image and pasting it into another region in the same image. This has placed several challenges in many fields. Therefore, detection of copy-move forgery in digital images is essential. In this paper, a fast copy-move forgery detection scheme using patch based descriptors is proposed.

Keywords— Copy-Move Forgery, Local Colour Feature, Adaptive Over-Segmentation, Forgery Region Extraction Algorithm.

I. INTRODUCTION

Digital images play a prominent role in authentication. Images are used to preserve integrity and authenticity. These images can be edited even by normal people, with the advancement of powerful graphics tools like Photoshop, Maya and so on. Manipulations of the images are done by the forgers with an aim to conceal or hide a part of the information. Nowadays, images are used in legal investigations, so one can presents tampered image to hide the truth. The forgery classifications are of different types [1]. Some of them are:-

i. Image Retouching:-In this method, the image details are reduced and the quality of the image is enhanced for attaining the attention from the readers.
ii. Image Splicing:-In this method, different elements from same images or different images are combined to form a single image.
iii. Copy-Move:-This method is the process of copying some part of region from an image and pasting it into another region in the same image.
iv. Image Morphing:- This method is used to transfer an object of one image into another.

Forgery detection approaches are classified into two. They are 1) Active Approach and 2) Passive Approach .In active approach, there are two approaches namely digital signatures and watermark. The active based approach has a drawback that a piece of information has to be inserted into the image before sending. The passive approaches are also known as blind approaches, it does not require any part of information about the image features as in the active approach. There are some other techniques like sharpening and blurring, noise variations, projective geometry and transformations etc. to detect the tampered image that uses the passive approach.

Cloning also known as copy-move forgery is the most common type of image forgery. Copy-move forgery detection classifications are of two types: (1) Block-based methods (2) Key-point based methods. In block-based methods, the image is first divided into overlapping and regular blocks and the forged region is detected by finding similar blocks. In key-point based methods, features are extracted from the entire block. In this method, there is no divisioning of images into blocks as in block based method. In terms of computational efficiency, space complexity and robustness against scaling and rotation, the key-point based methods are found better than the block based methods. But the key-point based method has some limitations also. Therefore, a new method based on a combination of the block-based methods and the key-point based methods is proposed.

II. RELATED WORKS

Fridrich et al [2] proposed a method based on DCT coefficients to detect the copy-move forgery in an image. In this method the image is divided into different overlapping blocks, and the features are extracted from each block. Each of the blocks are represented by quantized DCT coefficients and the blocks are lexicographically sorted. The forgery regions are detected by finding or locating similar blocks from the blocks sorted. Since, matching of mutual pairs are also considered, it results in the reduction of false matches. This method has a drawback that it results in false positives when the image has large identical texture.

Zhang et al [3] proposed a method to detect the copy-move forgery in digital images. The method is based on Discrete Wavelet Transform (DWT). In this, the low frequency band is divided into four non-overlapping sub-images. The phase correlation between every pair of the sub images is estimated. The region that has undergone tampering is detected by shifting the input image with respect to the estimated offset and subtracting the offset value from the input image. To detect the forged region the method adopts pixel matching. For highly compressed images the algorithm works well. Compared to other algorithms, this method has a lower computational time. If the copy-move forgery lies in more than one sub image the algorithm might fails.

S.J. Ryu [4] and his friends proposed an algorithm to detect the copy-move forgery in tampered images. This method extracts the features based on Zernike moments. Here, the suspicious image is first divided into blocks. Then from each block, a Zernike moment is calculated. The features that are computed are lexicographically sorted and the Euclidean distance between the pairs are estimated. The calculated Zernike moments has its magnitude that is invariant to rotation, JPEG Compression and blurring. This method identifies the forgery region by finding those blocks whose distance is smaller than the threshold set. This method fails in detecting the scaled copy-move blocks.

Amerini et al [5] proposed a SIFT-based detection algorithm that can detect and then estimate the geometric transformations that are used in the copy-move forgery. The detection involves three steps: in the first step, it extracts the SIFT features, and matches the key-points; the second step consists of key-point clustering and forgery detection, and in third step, the geometric transformations if any has occurred are estimated. The experimental results showed very good performance in terms of a high True positive ratio (TPR) and a low False Positive Ratio (FPR), even with JPEG compression and additive noise. Moreover, the results showed a high degree of precision in the estimate of the various parameters of the affine transformation.

A method based on SURF (Speeded Up Robust Features) is proposed by Bo et al [6]. This algorithm deals with the detection and description of interest points. This is a robust method that can be computed faster. Interest point detection involves finding stable interest points in an image and interest point description deals with generating descriptors for every interest points that are present in the detection step. This method is invariant to rotation. It uses a threshold value to enhance the robustness and to reduce the false detectors.

III. PROPOSED METHOD

A fast copy-move forgery detection scheme using patch based descriptors is proposed. In the existing methods, the image is divided into overlapping and regular blocks and the forgery is detected by using either of the block based methods or key-point based methods. Since the images are divided into overlapping and regular blocks, it fails to detect the forged regions accurately in many of the cases [7]-[9]. To detect the forged region accurately an Adaptive Over-Segmentation method is proposed [10]. Fig. 1 shows the framework of the proposed forgery detection scheme. First, the host image is divided into non-overlapping and irregular blocks. These blocks are called image blocks (IB). Then, Speeded Up Robust Features (SURF) algorithm is applied to each block to extract SURF feature points as Block Features (BF). These block features are matched with one another to detect the suspected forgery regions, and those features that matches successfully with one another is labelled as Labelled Feature Points (LFP). According to the extracted LFP, a Forgery Region Extraction method is proposed to detect the forgery region from the host image.

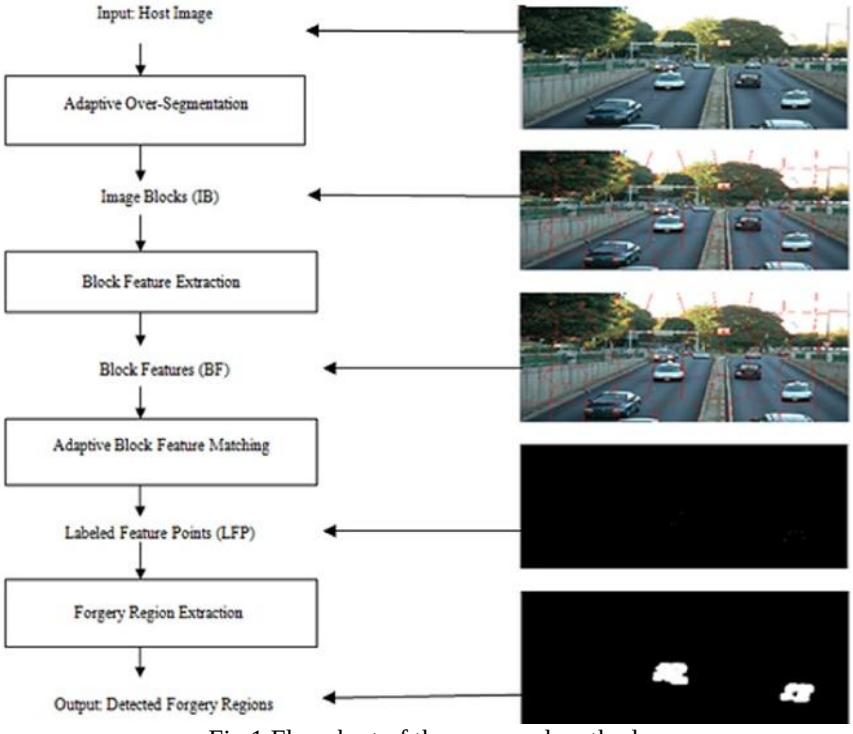

Fig.1 Flowchart of the proposed method

The proposed method involves the following steps. Each of them are discussed in detail:-

(i) SLICO Algorithm for Adaptive Over-Segmentation

In this paper, an Adaptive Over-Segmentation method is used in order to determine the initial size of the super pixels adaptively. There are a large amount of block based forgery detection algorithms so far. All of these existing methods divide the image into overlapping and regular blocks. The forgery regions are detected by matching those blocks. A four-level DWT is performed on the host image to find the relationship between the frequency distribution of the host images and the initial size of the super pixels. From this, the low frequency energy E_{LF} and the high frequency energy E_{HF} is calculated using the equations (1) and (2) respectively. Then, using the equation in (3) the percentage of the low frequency distribution P_{LF} is calculated.

$$E_{LF} = \sum |CA_4| \quad (1)$$

$$E_{HF} = \sum_i (\sum |CD_i| + \sum |CH_i| + \sum |CV_i|), i = 1,2,3,4 \quad (2)$$

In the above equations, CA_4 represents the approximation coefficients at the 4^{th} level of DWT and the CD_i ,CH_i and CV_i represents the detailed coefficients at the i^{th} level, where i = 1, 2, …,4.

$$P_{LF} = \frac{E_{LF}}{E_{LF} + E_{HF}} \cdot 100\% \quad (3)$$

The initial size S of the super pixels can be estimated using the equation in (4).

$$S = \sqrt{0.02 \times M \times N} \quad P_{LF} > 50\ \% \quad \text{or}$$
$$\sqrt{0.01 \times M \times N} \quad P_{LF} <= 50\ \% \quad (4)$$

In the above equation M x N represents the size of the image. Fig. 2 shows the flowchart of the Adaptive Over-Segmentation algorithm. In this method, to segment the host image as image blocks (IB), the initial super-pixel value obtained from equation (4) and SLICO algorithm is employed. The SLICO algorithm has an advantage that the user has no need to specify the compactness factor. Compared to Simple Linear Iterative Clustering (SLIC), algorithm, SLICO is fast and robust.

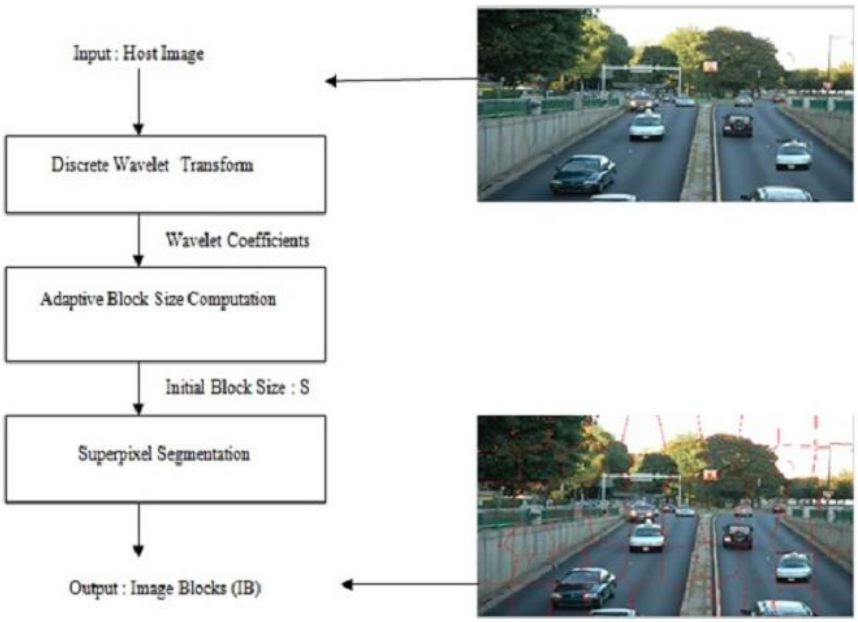

Fig. 2 Flowchart of the Adaptive Over-Segmentation algorithm.

(ii) Extracting Block Feature Using SURF Algorithm

Once the image blocks are obtained, block features (BF) are extracted from it. Nowadays, SIFT and SURF have been widely used in the field of feature extraction. These two algorithms are proven to be robust against common image processing operations like blurring, scale and compression. SIFT algorithm has more number of points compared to SURF and increases the accuracy whereas SURF results in lower computation time compared to that of the SIFT. As a result, we chose SURF as the feature point extraction method to extract the feature points from each block.

(iii) Extracting Labelled Feature Points by finding Matched Blocks

From the extracted block features (BF), the blocks that are having matches is estimated. For this, a block feature matching algorithm is proposed. In this method, the first step is to create a logical matrix for the matched blocks. Then the features are extracted from each of the blocks by comparing those blocks. Then an index pair is created to store the feature values. A threshold is to be set by trial and error method to check whether the blocks are having any matches or not. If there exists a matching between the blocks, then it is a forgery suspected region. When the blocks are matched, locate the x, y positions of those blocks and label the matched feature points in the matched blocks as Labelled Feature Points (LFP). Fig.3 shows the flowchart of extracting Labelled Feature Points (LFP).

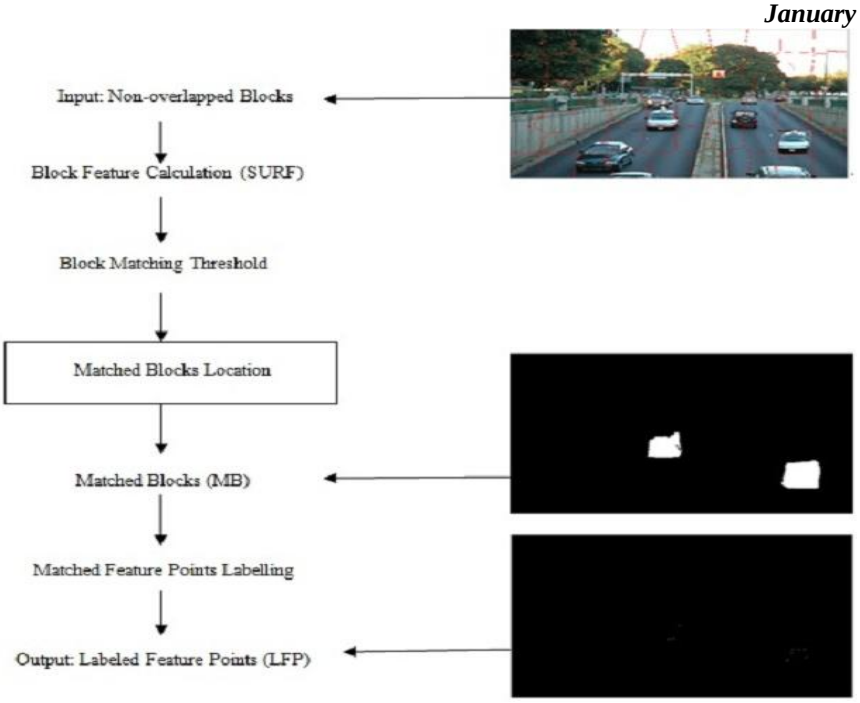

Fig.3 Flowchart of extracting LFP

Algorithm involves three steps:-
Input: Block Features (BF)
Output: Labelled Feature Points (LFP).

i. Load the Block Features $\{BF_1, BF_2, \ldots..BF_N\}$,where N is the number of image blocks.
ii. Locate the matched blocks (MB) as per the threshold set.
iii. The feature points that are matched in the matched blocks are then labelled to indicate the suspected forgery regions.

(iv) Forgery Region Extraction Algorithm

Once the labelled feature points (LFP) are extracted, there is a need to locate the forgery regions also. Since, this extracted LFP's are only the locations of the forgery regions. A Forgery Region Extraction algorithm is used to detect the forged regions more accurately. To obtain the suspected regions (SR), a method by replacing the LFP with the small super pixels is proposed. This is done by segmenting the host image very well as small superpixels. The local color features of the super-pixels that are neighbors of the suspected regions (SR) are also measured to improve the precision and recall rates. When this local color feature is same as that of the suspected regions, then the neighbor super pixels are merged into the corresponding suspected regions. This merging process results in merged regions (MR). Finally, to generate the detected copy-move forgery regions, morphological operation is applied to this merged region. Fig.4 shows the flowchart of the Forgery Region Extraction Algorithm.

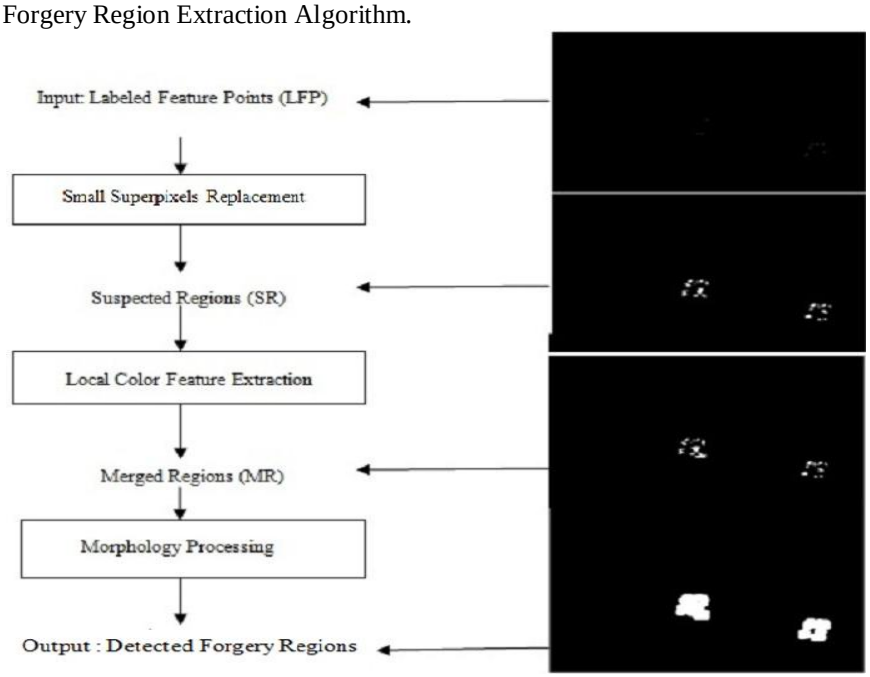

Fig.4 Flowchart of the Forgery Region Extraction Algorithm

Algorithm involves three steps:-

Input: Labeled Feature Points (LFP)

Output: Detected Forgery Regions.

i. Load the Labeled Feature Points (LFP), and then segment the host image into small superpixels as feature blocks by applying SLIC algorithm with the initial size S and replace the LFP with these superpixels to generate the Suspected Regions (SR).
ii. Calculate the local color features of the superpixels that are neighbors of the suspected regions (SR). When the local color features of the neighbor blocks and the suspected regions are similar, then merged regions is generated.
iii. Finally, to generate the detected forgery regions apply the morphological operation.

In step (i) , assume that LFP = { { $LP_1, \overline{LP_1}$ }, { $LP_2, \overline{LP_2}$ }…..,{ $LP_n, \overline{LP_n}$ } }, where { $LP_i, \overline{LP_i}$ } represents a matched feature point pair, here i is the i^{th} labelled feature point pair, i = 1,2,……,n, and n represents the total number of feature points in the LFP; the suspected regions will be SR = {{ $LS_1, \overline{LS_1}$ }, { $LS_2, \overline{LS_2}$ }, ….., { $LS_n, \overline{LS_n}$ } }. To segment the host image into small super-pixels with the initial size of the super pixel SLIC algorithm is used.

In step (ii), the neighboring blocks are defined as SR_i_neighbor = $\left\langle LS_{i\_\theta}, \overline{LS_{i\_\theta}} \right\rangle$, where θ = {$45^0$, 90^0, 135^0, 180^0, 225^0, 270^0, 315^0, 360^0} for each suspected region SR_i = $\left\langle LS_i, \overline{LS_i} \right\rangle$. Using the equations in (5) and (6) the local color feature of the suspected region SR_i and its neighboring blocks SR_i _neighbor is measured.

$$F_{C\_LS_i} = \frac{R(LS_i) + G(LS_i) + B(LS_i)}{3}$$

$$F_{C\_\overline{LS_i}} = \frac{R(\overline{LS_i}) + G(\overline{LS_i}) + B(\overline{LS_i})}{3} \quad (5)$$

$$F_{C\_LS_{i\_\theta}} = \frac{R(LS_{i\_\theta}) + G(LS_{i\_\theta}) + B(LS_{i\_\theta})}{3}$$

$$F_{C\_\overline{LS_{i\_\theta}}} = \frac{R(\overline{LS_{i\_\theta}}) + G(\overline{LS_{i\_\theta}}) + B(\overline{LS_{i\_\theta}})}{3} \quad (6)$$

Where R (), G () and B () is the calculation of RGB components of the corresponding blocks respectively and $F_{C\_LS_i}$ and $F_{C\_\overline{LS_i}}$ are the local colour features of the suspected regions SR_i and $F_{C\_LS_{i\_\theta}}$ and $F_{C\_\overline{LS_{i\_\theta}}}$ is the local colour features of the neighbour blocks SR_i _neighbour. If the local colour feature of the neighbouring block is similar to that of the suspected regions merged regions are generated. This is done by setting a threshold using the trial and error method. Finally, in step (iii), a morphological operation is to be applied to generate the detected forgery regions. By doing this, a forged region can thus be detected more accurately.

IV. CONCLUSIONS

The proposed method integrates both the block-based method and the key-point based method. First, an adaptive over-segmentation algorithm is proposed to segment the host image into a non overlapped and irregular block adaptively. Since, SURF algorithm is employed to detect the feature points, the computational time can be reduced. Moreover, in this method, to detect the forged regions more accurately a Forgery Region Extraction algorithm is also proposed. With all of these, the proposed scheme is expected to be more efficient than that of the existing ones.

ACKNOWLEDGMENT

I am thankful to Ms. Veena Viswam, Assistant Professor of Computer Science and Engineering Department, KMEA for her keen interest and guidance in my paper.

REFERENCES

[1] Salam A Thajeel, Ghazali Sulong, " A Survey of Copy-Move forgery detection techniques," in Journal of Theoretical and Applied in Journal of Theoretical and Applied Information Technology,Vol.70 No.1,December 2014.

[2] J. Fridrich, D. Soukal, and J. Lukas, "Detection of copy–move forgery in digital images," in Proc. Digit. Forensic Res. Workshop, Cleveland, OH, Aug. 2003.

[3] J. W. Wang, G. J. Liu, Z. Zhang, Y. W. Dai, and Z. Q. Wang, "Fast and robust forensics for image region-duplication forgery," Acta Automat. Sinica, Vol. 35, no. 12, pp. 1488–1495, 2009.

[4] S. J. Ryu, M. J. Lee, and H. K. Lee, "Detection of copy-rotate-move forgery using Zernike moments," in Information Hiding. Berlin, Germany: Springer-Verlag, pp. 51–65, 2010.hg

[5] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFT-based forensic method for copy–move attack detection and transformation recovery," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 1099–1110, Sep. 2011.

[6] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, "Image copy–move forgery detection based on SURF," in Proc. Int. Conf. Multimedia Inf. Netw. Secur. (MINES), pp. 889–892, Nov. 2010,.

[7] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Dept. Comput. Sci., Dartmouth College, Hanover, NH, USA, Tech. Rep. TR2004-515, 2004.

[8] W. Luo, J. Huang, and G. Qiu, "Robust detection of region-duplication forgery in digital image," in Proc. 18th Int. Conf. Pattern Recognit. (ICPR), Aug. 2006, pp. 746–749.

[9] S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy–move forgery," in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP), Apr. 2009, pp. 1053–1056.

[10] Chi-Man Pun, Xiao-Chen Yuan, "Image Forgery Detection Using Adaptive Over-segmentation and Feature Point Matching", IEEE Transactions on Information Forensics and Security, Vol.10,No.8, August 2015.

