DETECTION OF COPY-MOVE IMAGE FORGERY USING WAVELET TRANSFORM AND VISUAL DESCRIPTOR FEATURES

[1]J. Thilagavathy, [2]M.Arul mozhi mari thayammal
[1]Assistant professor, Department of Electronics and Communication Engineering,
Grace College of Engineering, Thoothukudi.
[2]PG student, Department of Electronics and Communication Engineering,
Grace College Of Engineering, Thoothukudi

ABSTRACT

Copy-move image forgery is one type Of image forgery where a part of the image is copied and then it is pasted in the same image to hide or add some important object(s) within the image. Most image forgery detection models are unable to detect forgery in the image if the copied portion has noise or it is rotated or scaled before pasting.. Firstly, the image is converted to gray scale. Discrete Wavelet Transform (DWT) is used to decompose the gray scale image into four parts and Scale Invariant Feature Transform(SIFT) algorithm is used to extract the key-points from the approximate part of the decomposed image. Using parallel matching take the decision whether the image is forgery or not. The proposed model shows 96% accuracy over a certain dataset of images.

Key words: Discrete Wavelet Transform, Scale Invariant Feature Transform algorithm, parallel matching, Simple Linear Iterative Clustering.

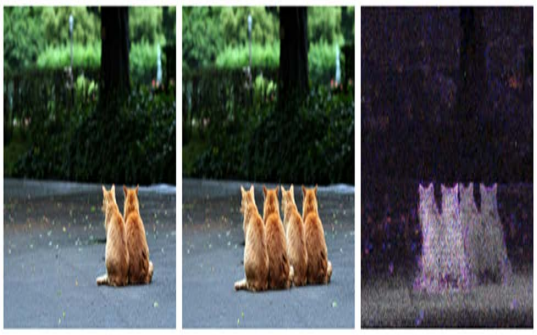
I. INTRODUCTION

Digital image is a memorandum of precious moments of human life. It expresses vast amount of pictorial information like a witness. Hence, imagery information is used as a vital proof against various types of crime and acts as evidence for multifariouspurposes. However, the availability of many image editing software and tools has made image manipulation easier. This process of manipulation of original image by applying various types of geometric transformations, adding or removing an object in the real image is called digital image forgery [1]. To ensure the authenticity of image, there are many algorithms and models that are being developed to solve this issue. However, most of these models have limitations either in time complexity or in detection accuracy. So, the detection system should overcome these limitations and difficulties.

Digital image forgery detection can be classified into two major categories: active method and passive method [2,3]. In active method some preprocessed digital information like signature or watermarking is embedded in the image. However, most of the digital images that have already been created are not authenticated with embedded information. As a result, we need a different method that helps to verify authenticity without any prior information. This requirement is satisfied by passive approach of image forgery detection. There are a number of ways to identify image tampering using passive method while at the same time there are various ways to tamper an image such as retouching, splicing, enhancing, copy-move(cloning) etc. [5]. In copy-move image forgery, a part of image is copied and then it is pasted in the same image having an intention to make a false image or hide some important object within the image [4]. The goal of this proposed method is to detect image forgery irrespective of all the ways of copy-move tampering including tampering with geometric transformation giving importance to reduce time complexity. The outline of the

proposed model of this paper follows this sequence: section ii presents related work of existing detection methods for digital image tampering. Section iii presents detailed description of algorithms required for the implementation of proposed model. Section iv presents experimental result and performance analysis of proposed model. Section v presents conclusion and future work.Example for Forgery

- Copy-Move manipulation is typically done to make an object' disappear' from the original image by covering it with a small fragment copied from another part of the same image.
- This method is also used to duplicate existing objects in the picture.



II. Existed system

In this existing system copy-move forgery detection scheme which can accurately localize duplicated regions with a reasonable computational cost. In existed system detect forgery object new interest point detector algorithm is used utilizing the advantages of both block-based and traditional keypoint-based methods. The detected key points adaptively cover the entire image, even low contrast regions, based on a uniqueness metric. Moreover, a filtering algorithm is employed which can effectively prune the falsely matched regions. Considering the new interest point detector, an iterative improvement strategy is used.

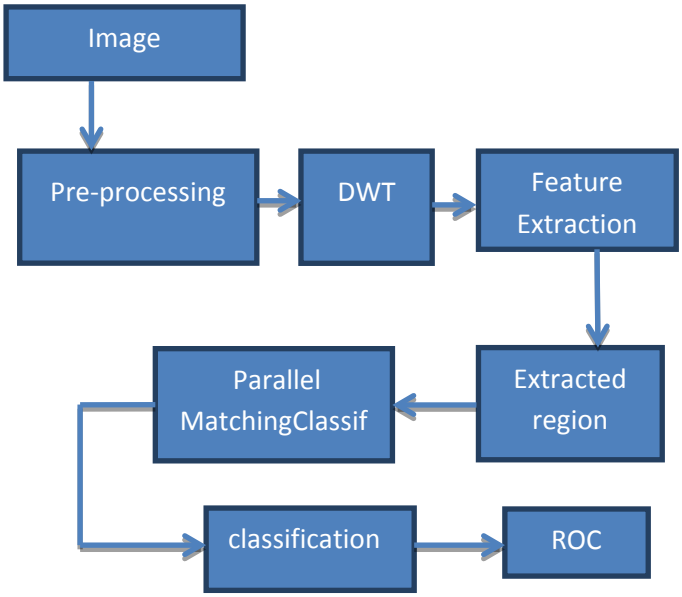
Drawback

- Medium accuracy of filter algorithm
- Execution time high
- Need more performance.

III. Proposed system

In this project, we propose a novel copy-move forgery detection scheme which can accurately localize duplicated regions with a high accuracy. The purpose of proposed method is to detect copy-move forgery in digital image. First, the input image is decomposed with DWT which is later and segmented with Simple Linear Iterative Clustering. After segmented image extract key-point features by applying SIFT. The extracted feature is used to form clusters which help to find matching between copied and forged region. We use parallel matching algorithm used purpose of improve speed of the system. To get the final result of matching outliers are removed. We applying an algorithm for collection of forgery and non-forgery images. Finally our algorithm classifies the forgery and non-forgery images with high accuracy.

Block Diagram



Working Principle

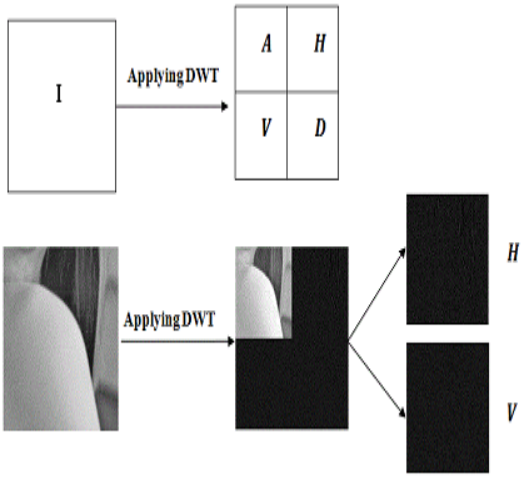
We proposed a new model specifically designed for CMFD. The model comprises of four sub steps. Firstly, the input image is segmented with DWT and Simple Linear Iterative Clustering. Segmented area extracts Visual descriptors like SIFT algorithm. Using Parallel computing matching model works detecting the forgery areas. Finally we can be classify the forgery and non-forgery images.

Pre-processing

The preprocessing step of the model comprises of two sub-steps. Firstly, the input image is converted to grayscale if it is a RBG image. The reason behind converting it into grayscale is to reduce complexity by converting a 3D pixel value (R, G, B) to a 1D value. Besides the color information does not contribute in identifying key-point features. The following formula is used to convert the RGB values to grayscale value.

$Y = 0.2989R + 0.5870G + 0.1140B$

Secondly, DWT is used to obtain four sub bands such as approximate (DWA), horizontal (DWH), vertical (DWV), diagonal(DWD).



The approximate sub band is later passed as input parameter in SIFT algorithm to extract key-points features. The primary reason for choosing DWT is that it is shift invariant, translation invariant and efficient at finding similarities and dissimilarities despite of having noise or blurring in the image.

SLIC (Simple Linear Iterative Clustering) Algorithm for Superpixel generation

A superpixel can be defined as a group of pixels that share common characteristics (like pixel intensity). Superpixels are becoming useful in many Computer Vision and Image processing algorithms like Image Segmentation, Semantic labeling, Object detection and tracking etc. because of the following-

They carry more information than pixels.Superpixels have a perceptual meaning since pixels belonging to a given superpixel share similar visual properties. They provide a convenient and compact representation of images that can be very useful for computationally demanding problems.

This algorithm generates superpixels by clustering pixels based on their color similarity and proximity in the image plane. This is done in the five-dimensional [labxy] space, where [lab] is the pixel color vector in color space and xy is the pixel position. We need to normalize the spatial distances in order to use the Euclidean distance in this 5D space because the maximum possible distance between two colors in the CIELAB space is limited whereas the spatial distance in the xy plane depends on the image size. Therefore, In order to cluster pixels in this 5D space, a new distance measure that considers superpixel size was introduced.

SIFT Feature Extraction

SIFT is one of the best feature extracting algorithm proposed by David Lower. It is invariant to image rotation, geometrical transformation, intensity and change of viewpoint in matching features.

In this step Gaussian of Difference (DoG) is used to find possible points of interest which are invariant to orientation and scaling. To make the detection of key-points more reliable, efficient and stable DoG Function D (x, y, σ) is required.The key-points that are initially identified on the approximate component of decomposed image.

Key-point Matching

The extracted key-points from SIFT algorithm are used to find a pool of matching pairs of key-points. Euclidian distance is computed for finding the matched pairs of key-points from a certain key-point to remaining key-points. This process repeats iteratively and based on pre-defined threshold value a set of matched pairs are identified.

IV. RESULTS

Fig.1 Input Image

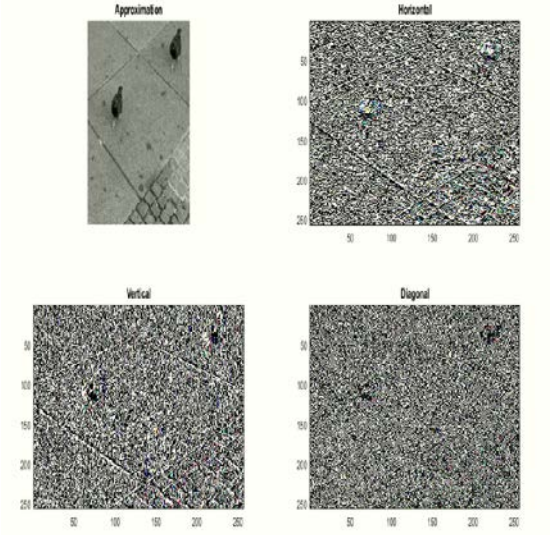


Fig.2 DWT Image

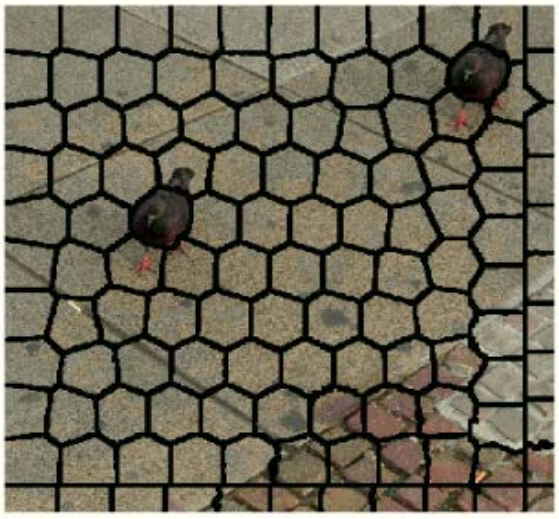


Fig.3 SLIC Image

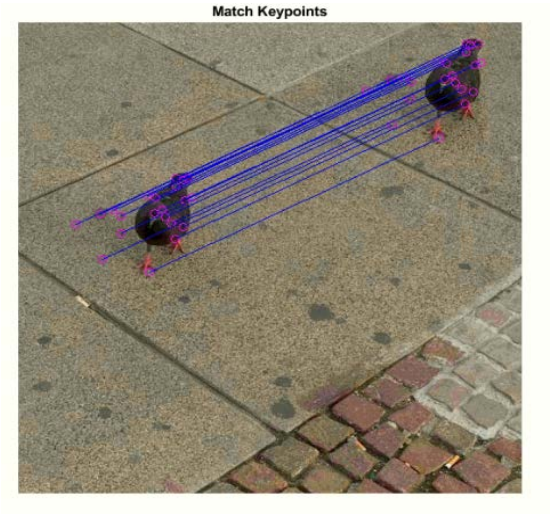


Fig.4 Key points matching

Fig.5 Extract forgery points Image

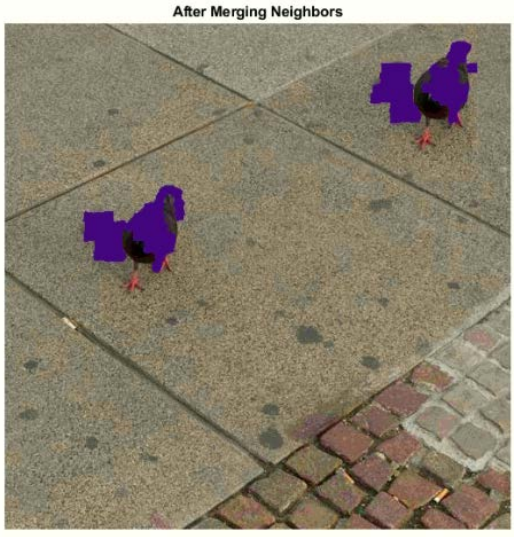


Fig.6 Morphological merging neighbors Image

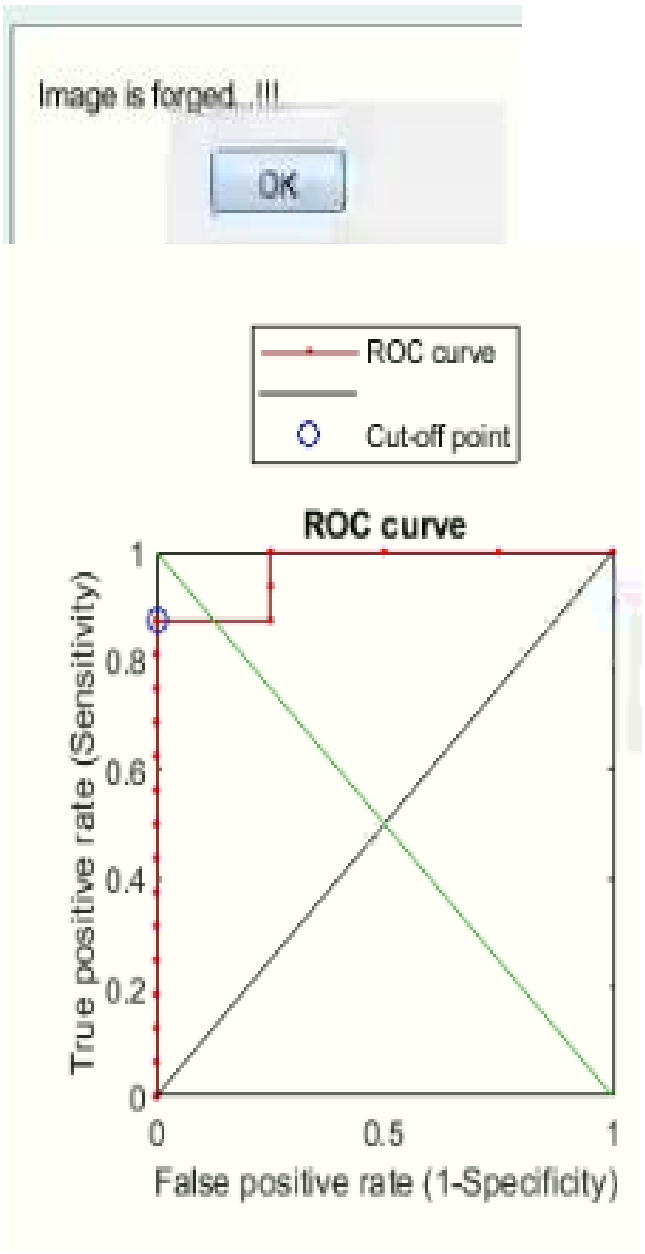


Fig.7 ROC graph image

V. Conclusion

This project presents a robust key-point based copy-move forgery detection method in digital image by applying the DWT decomposition technique with SLIC methodandSIFTfeature extraction algorithm. DWT is shift invariant, blur and noise invariant. With the simulation performed on original and copied images, it shows that DWT and SIFT perform better in terms of time complexity and accuracy. From the performance analysis and experimental result it is evident that the proposed model shows better accuracy and efficiency than other existing copy-move forgery detection techniques. In our future work, we will improve the detection technique reducing the false positive rate and increasing percentage of accuracy.

VI. ACKNOWLEDGEMENT We express immense gratitude to our Guide Prof. J. Thilagavathy for her support and encouragement. We also especially thank herfor her useful suggestions and having laid down the foundation for the success of this work.

VII. Reference

1. Khan, U. A., Kaloi, M. A., Shaikh, Z. A., & Arain, A. A. (2018). A Hybrid Technique for Copy-Move Image Forgery Detection. 2018 3rd International Conference on Computer and Communication Systems (ICCCS).
2. Bi, X., Pun, C.-M., & Yuan, X.-C. (2016). Multi-Level Dense Descriptor and Hierarchical Feature Matching for Copy–Move Forgery Detection. Information Sciences, 345, 226–242.
3. Jian Li, Xiaolong Li, Bin Yang, & Xingming Sun. (2015). Segmentation-Based Image Copy-Move Forgery Detection Scheme. IEEE Transactions on Information Forensics and Security, 10(3), 507–518.
4. Muzaffer, G., Erdol, E. S., & Ulutas, G. (2018). A copy-move forgery detection approach based on local intensity order pattern and patchmatch. 2018 26th Signal Processing and Communications Applications Conference (SIU).
5. Dixit, R., Naskar, R., & Sahoo, A. (2017). Copy-move forgery detection exploiting statistical image features. 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET).
6. Weiqi Luo, Jiwu Huang, Guoping Qiu, “Robust Detection of Region-Duplication Forgery in Digital Images”, In proceedings of the International Conference on Pattern Recognition, Washington, DC, pp. 746-749, 2006.
7. Weihai Li and Nenghai Yu, “Rotation Robust Detection of Copy-move Forgery”, In proceedings of the IEEE 17th International Conference on Image Processing, Hong Kong, 2010.
8. Yanping Huang, Wei Lu, Wei Sun and Dongyang Long, “Improved DCT-based Detection of Copy-Move Forgery in Images”, Forensic Science International, vol. 206, pp. 178-184, 2011.

9. Yanjun Cao, Tiegang Gao, Li Fan, Qunting Yang, "A robust detection algorithm for copy-move forgery in digital images", Forensic Science International, vol. 214, pp.33–43, 2012.
10. http://www.cs.albany.edu/~xypan/research/duplication/main.html
11. V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An Evaluation of popular copy-move forgery detection approaches," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 6, pp. 1841–1854, Dec. 2012.
12. H. Huang, W. Guo, and Y. Zhang,"Detection of copy-move forgeryin digital images using sift algorithm," in *Proc. Pacific-Asia WorkshopComputational Intell. and Industrial Applicat. (PACIIA)*, vol. 2, 2008,pp. 272–276.
13. 13. S. J. Nightingale, K. A. Wade, and D. G. Watson, "Can people identify original and manipulated photos of real-world scenes?" Cognitive research: principles andimplications, vol. 2, no. 1, p. 30, 2017.