International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 4
ISSN: 2454-4248
680 – 684

Wavelet-based Image Splicing Forgery Detection

[1]Tulsi Thakur
M.Tech (CSE) Student, Department of Computer Technology, YCCE, Nagpur, India
e-mail: basiltulsi@gmail.com

[2]Dr. Kavita Singh
Head & Associate Professor, Department of Computer Technology, YCCE, Nagpur, India
e-mail: singhkavita19@yahoo.com

[3]Mr. Arun Yadav
Tata Consultancy Services (TCS), Mihan, Nagpur, India
e-mail: arun.yadav@tcs.com

[4]Dr. M. M. Raghuwanshi
Professor, Department of Computer Technology, YCCE, Nagpur, India
e-mail: m_raghuwanshi@rediffmail.com

***Abstract*—**Digital image processing is a progressive field which has made development over period of time in a way that it becomes easy to play with artifacts of image by manipulating them using transformation such as copy-paste, copy-move, rotation, smoothing of boundaries, scaling, color enhancing, resizing, addition of noise, blurring, compressing etc. Forgery performed with a digital image, raising a doubt about the authenticity of it. Image splicing is one of the most used method for tampering an image by compositing two or many image fragments to create a spliced image. In this paper, a wavelet-based mechanism is proposed to detect image splicing forgery by taking edge information of an image as a distinguishing feature by performing edge analysis using wavelet transform. Haar-based Discrete Wavelet Transform (DWT) is used for edge analysis that decompose an image into four sub-images and it followed by Speed-Up Robust Feature (SURF) method which is a keypoint-based feature extractor technique. SURF extracts features from the decomposed images of DWT and used that features for performing classification using SVM linear classifier.

Keywords- *Image splicing forgery, DWT, SURF, SVM*

*****

I. INTRODUCTION

Images are an impressionable way to share information as there is belief that picture speaks louder than words. Development in the area of image processing technology made possible the journey of image from paper to camera and now to mobile. Extensively grown area of image editing tools made easy to perform fraudulent activities with images and a forged image can lead misguiding to take decisions as digital images are all over the internet and day-to-day life. There are many approach to perform manipulation with image though image splicing is the frequently used method. Image splicing combines the two or many fragments of image to create single spliced image by cut and paste image fragments from different images to one image [1][2]. Forged image can be indistinguishable from the authentic image.

Image splicing forgery detection is a crucial job due to numerous techniques available for alter the digital image and different image capturing devices. Commonly image forgery detection method is categorized into two approaches viz; an active approach and passive approach [1][2][3]. Active approach is based on data embedding like digital signature attachment or watermark embedding while taking picture or before distribution. However, passive approach does not work with data assignment on image, rather it works with the evidences leave behind in image while tampering. Image splicing detection is fall under the passive approach for image forgery detection method as it works on the footprint left while creating spliced image. Features such as abrupt changes in edges, noise variance, spectral and textural features, statistical discrepancies, change in sensor noise pattern, change in lighting direction blurred type inconsistency can be use as distinguishable evidence of forgery done with digital image [4].

In the work, a passive approach mechanism for image splicing forgery detection is proposed for identifying the given image as authentic image or forged one. The proposed mechanism is based on wavelet transform to detect image splicing forgery by analyzing edges of image using Haar-based Discrete Wavelet Transform (DWT). Decomposition of an image is accomplished using DWT transform, which decomposed image and obtained four sub-images viz; LL, LH, HL and HH. Although, these DWT coefficients are eventually approximation image, horizontal detail image, vertical detail image and diagonal detail image respectively. Decomposition of image is followed by feature extraction using Speed-Up Robust Feature (SURF) that extracted features from each sub-image of decomposed image. SURF is keypoint-based feature extractor as well feature descriptor, which store additional information of an image such as surrounding pixel values of the extracted keypoint. Descriptor helps in identifying the keypoint surrounding pixel values abnormality and shows robustness against geometric transformation like scaling and rotation. SURF extracted interest keypoint from decomposed image and generated a descriptor i.e., feature vectors to store the information of extracted features. These feature vectors contained the information of position of interest point, that further supplied to SVM classifier. Images are classified into spliced or authentic image using SVM classifier for classification.

 ISSN: 2454-4248
680 – 684

The rest of the paper is organized as follows. An introductory discussion on image splicing forgery and detection is carried out in section I. Section II presents proposed methodology for image splicing forgery detection using Haar-based wavelet. In section III provides experiments analysis and section IV gives conclusions and scope of the future work.

II. PROPOSED METHOD

The proposed mechanism analyses the abrupt changes occurred in edges of an image for image splicing forgery detection. It mainly consists of decomposition of image using DWT to catch the inconsistency in edges and further followed by feature extraction performed by SURF feature extractor on decomposed image through DWT. Extracted features are used by Support Vector Machine (SVM) for classification. The proposed mechanism detects image splicing forgery in an image and also shows the forged region in an image. Figure 1 presents the flow of the proposed mechanism to identify splicing in an image.

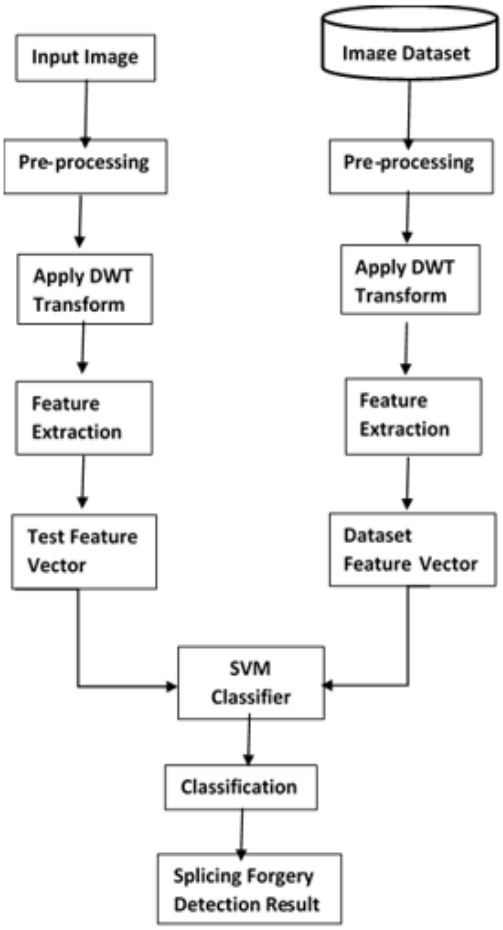


Figure 1: Proposed Image Splicing Forgery Detection Mechanism

A. *Wavelet Decomposition*

Discrete Wavelet Transform (DWT) is transform image into time- frequency domain. Transforming an image to time-frequency domain gives a representation to investigate transient, time-variant (*i.e.*, non-stationary) signal to analyze the region of discontinuities *i.e.*, a feature that is for specific images those are having discontinuities at edges. When DWT decompose an image to get four sub-image namely LL, LH, HL and HH [5]. LL depicts to coarse level coefficient or as an approximation image of half-sized version of original image that include almost all information of actual image and LH, HL and HH depicts the detail coefficients or image that provides edge information of image and contains horizontal, vertical and diagonal coefficient respectively [6].

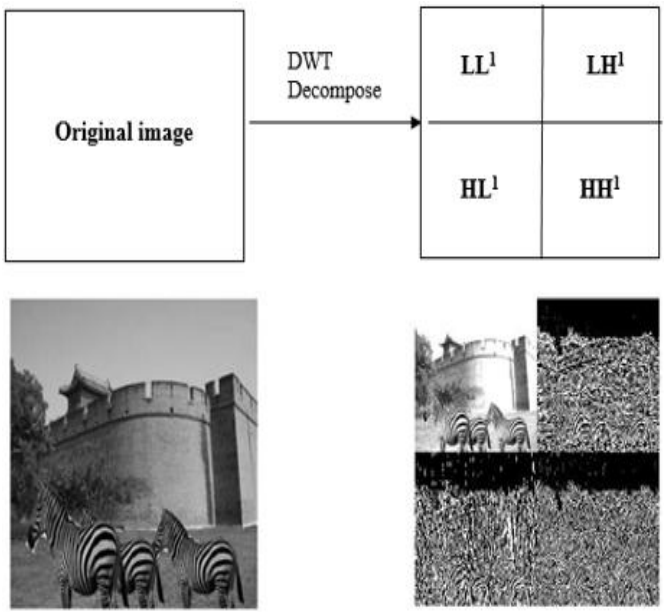


Figure 2: A level DWT Decomposition

In figure 2, one level DWT transform applied on image that decomposed it and obtained four sub-images viz; LL, LH, HL and HH. These coefficients depict approximation and detail values. Low-pass sub-image containing coarse approximation information of the source image labeled as LL and three high-pass sub-images that generates image details through different directional details of image that are LH, HL and HH are horizontal, vertical and diagonal coefficients that corresponds to giving horizontal, vertical and diagonal edge information of an image. These coefficients are useful in finding the pasted region boundary edges occurred during image splicing forgery. Image splicing forgery detection is use finding weak edge boundary of pasted region while preserving strong edges of image. DWT analyzes weak edges and preserves strong edges by decomposing image into multi-resolution image.

 ISSN: 2454-4248
680 – 684

When DWT decompose an image of size 2i × 2i pixels, Low Pass Filter (LPF) and High Pass Filter (HPF) downscales to size 2i/2 × 2i/2 pixels of image x(n) to get horizontal approximation image that gives almost all information of original image and horizontal detail image gives horizontal details about an original image. Further, on horizontal approximation image again LPF and HPF applied to get sub-images like LL and LH that are giving low resolution approximate image and horizontal image. Similarly, Horizontal detail image is decomposed to get sub-images HL as well as HH that are depicting high resolution vertical detail image and diagonal detail image as presented in figure 3.

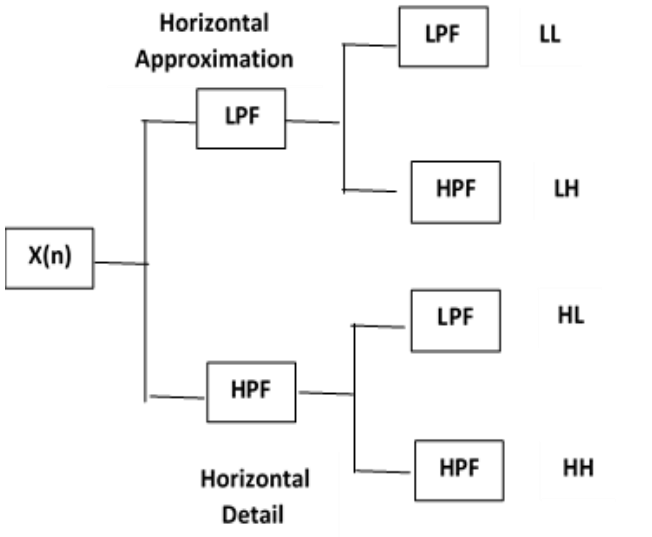


Figure 3: DWT Decomposition

B. Feature Extraction

The process of feature extraction is inspecting an image to detect interesting features that are distinctive to the objects in the digital image in a way that it will help to detect an object that is not a part of original image. Image splicing commonly changes image characteristics and abrupt and inconsistent edges occurred due to forgery. These introduced edges from original image edge can be essential evidence in image splicing detection.

Speed-Up Robust Feature (SURF) is a feature extractor and descriptor method that is based on blob-based keypoint feature extraction. Robustness of local feature make SURF more reliable that extracts interesting keypoint features from the image [8]. SURF works on local feature pixels as local features tell about the changes occurred at pasted region boundary. In proposed mechanism, SURF is applied on decomposed image through DWT to extract features from all sub-images. The extracted SURF features are plotted on an image as shown in the figure 4 and it depicts the extraction of features from all the sub-images of DWT decomposed images. In figure 4, A Image corresponds to approximation image and extracted features from the A image has been shown. H Image depicts the horizontal image in figure 4 that shows the extracted features point from the horizontal image detail and similarly V Image and D Image presented the extracted keypoint from the vertical and diagonal sub-image. The area of zebras is a spliced region in authentic image and SURF has extracted keypoint around that region as shown in figure 4.

In training phase, created database images are processed by DWT and further decomposed images are given to SURF to extract features from all images that are belong to database. SURF extracted the features from all decomposed images and also generated a descriptor for each extracted features and store it as feature vector in database.

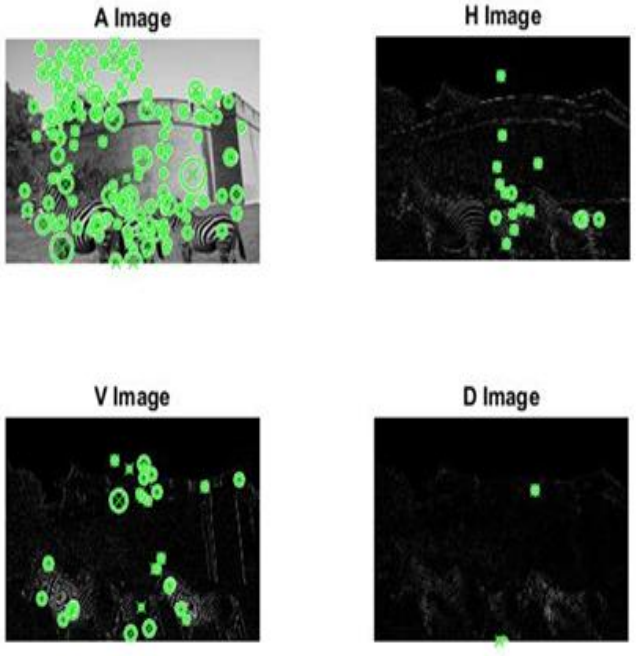


Figure 4: Extracted Features using SURF

III. Experimental Results

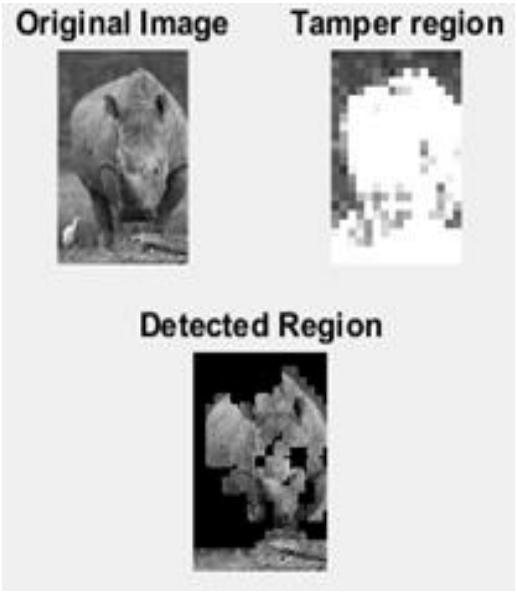
The proposed mechanism is detected image splicing and detected forged region in an image as shown in figure 5. This Image splicing forgery detection mechanism is evaluated on a publically available dataset for image forgery detection: CASIA v1.0 Tampered Image Detection Evaluation Database which contains variety of images containing categories scene, plant, animal, texture, *etc.* and images are categorized into two classes *i.e.*, Authentic image set and Spliced image set.

 ISSN: 2454-4248
680 – 684

For classification SVM classifier is used. In the proposed method, SURF is not restricted to number of features limit and as each image has different number of features, SURF extracted variable length of features from the decomposed images. To deal with variable length features multiple SVMs concept has been used. As SVM works on fixed length features, In the proposed method multiple SVMs are created. To train an SVM with 300 images using multiple SVM concept, it obtained 10 trained SVMs that save all features value and their classes belonging of the images.

The proposed mechanism detected image splicing forgery in an image as depicted by figure 5 that shows output of the proposed method in figure 5(b), when it experiments on the forged image as depicted in figure 5(a). Output contained the tampered region localization and detected the spliced region area in a given forged image as well as localized it the forged region in an image.

(a) Input Image



(b) Output

Figure 5: Detected image splicing forgery

Figure 6 presented the experimental analysis performed on the proposed mechanism to detect image splicing forgery in an image with measure parameter such as true positive, false positive, true negative and false negative.

- True Positive (TP): A forged image that is classified as a forged image.
- False Positive (FP): An authentic image that is classified as a forged image.
- True Negative (TN): An authentic image that is classified as authentic image.
- False Negative (FN): An forged image that is classified as an authentic image.

Accuracy is the term shows the proposed mechanism is correctly classified images given to the mechanism. It obtained 87.5% accuracy, which explains that the proposed mechanism is giving good accuracy rate and detected forgery in an image.

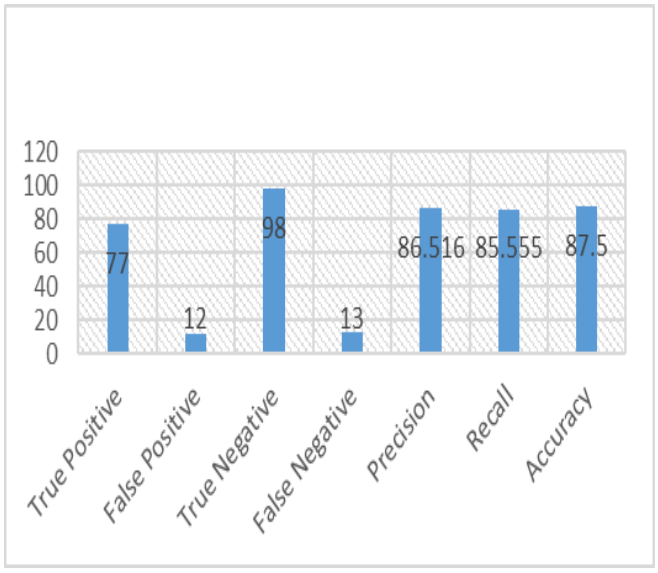


Figure 6: Experimental analysis on the proposed mechanism

IV. CONCLUSIONS

The proposed work has been introduced wavelet-based image splicing forgery detection mechanism with SURF feature extractor. It is mainly focused approach on image splicing forgery detection in an image to verify the integrity of image. SURF works on local feature pixels as local features tell about the changes occurred at pasted region boundary. Using SURF feature extractor interesting keypoint has been extracted. The proposed mechanism detected forgery in the image and

 ISSN: 2454-4248
680 – 684

localized the forged region in image. Wavelet transform analyzed inconsistency in image that gives the changes occurred in the images and abrupt changes in edges helped to detect forgery in the image. As per experimental observations performed on CASIA v1.0 dataset, 87.5% accuracy has been attained by the proposed method. However, SURF features are invariant to scale and rotation transformations, thus SVM classifier performed well and has been given good accuracy, precision along with recall and fast classification of images. The outcome of this proposed work is to authenticate an image that is helpful in various field of day to day life.

REFERENCES

[1] V. P. Nampoothiri and N. Sugitha, "*Digital Image Forgery - A threaten to Digital Forensics"*, IEEE International Conference on Circuit, Power and Computing Technologies (ICCPCT), pp. 1-6, 2016.

[2] C. N. Bharti and P. Tandel, "*A Survey of Image Forgery Detection Techniques"*, IEEE International conference on Wireless Communication, signal Processing and Networking, pp. 877-881, 2016.

[3] T. S. Thakur, K. R. Singh and A. Yadav, "*Blind Approach for Digital Image Forgery Detection*", International Journal of Computer Applications (IJCA), Vol. 179, No.10, pp. 34-42, 2018.

[4] M. M. Isaaca and M Wilscy, "*Image forgery detection based on Gabor Wavelets and Local Phase Quantization*", ELSEVIER Second International Symposium on Computer Vision and the Internet (VisionNet'15), pp. 76-83, 2015.

[5] A. Kashyap, R. S. Parmar, B. Suresh, M. Agarwal and H. Gupta, "*Detection of Digital Image Forgery using Wavelet Decomposition and Outline Analysis*", International Conference of Signal Processing and Communication (ICSC), pp. 187-190, 2017.

[6] W. Wang, J. Dong and T. Tan, "*Effective Image Splicing Detection Based on Image Chroma*", IEEE International Conference on Image Processing (ICIP), pp. 1257-1260, 2009.

[7] M. F. Hashmi, A. R. Hambarde and A. G. Keskar, *"Copy Move Forgery Detection using DWT and SIFT Features*", IEEE International Conference on Intelligent Systems Design and Applications (ISDA), pp. 189-193, 2013.

[8] Herbert Bay, Andreas Ess, Tinne Tuytelaars, and Luc Van Gool, "*Speeded-Up Robust Features (SURF)",* Preprint submitted to Elsevier, pp. 1-14, 2008.

[9] The dataset mentioned in the paper is freely available to reader at the address [online]. Available: http://forensics.idealtest.org/casiav1/