A Robust Method for Detecting Copy-Move Image Forgery Using Stationary Wavelet Transform and Scale Invariant Feature Transform

Taposh Das
Computer Science and Engineering
BRAC University
Dhaka, Bangladesh
e-mail:taposh24x7@gmail.com

Md. Rasel Azam
Computer Science and Engineering
BRAC University
Dhaka, Bangladesh
e-mail:raselazam23@gmail.com

Rizbanul Hasan
Computer Science and Engineering
BRAC University
Dhaka, Bangladesh
e-mail:rizbanulhasan08@gmail.com

Jia Uddin
Computer Science and Engineering
BRAC University
Dhaka, Bangladesh
e-mail: jia.uddin@bracu.ac.bd

***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. The purpose of this paper is to propose a robust and efficient detection technique for this kind of image forgery. Firstly, the image is converted to grayscale. Then two-level Stationary Wavelet Transform (SWT) is used to decompose the grayscale 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. Later, the matched pairs of key-points are identified. Then matched pairs of key-points are clustered using several linkage methods. Clustered key-points are compared to take the decision whether the image is tampered or not. In the post-processing step, false positive matches are removed using Random Sample Consensus (RANSAC). The proposed model shows 93% accuracy over a certain dataset of images.**

Keywords—SIFT; SWT; key-point descriptor; RANSAC; copy-move image forgery

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 multifarious purposes. 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.

II. Related Work

In [6,9,12] authors propose a key-point based copy-move forgery detection method. In SIFT and SURF based approach key-point feature is extracted to form key-point descriptor vector that later is used to form clusters for matching forged regions. In HOG based approach, 1-D DWT is used to get the approximate image that is subdivided into smaller blocks and later every block is used to find HOG features which are then similarly used for forming clusters for matching tampering region.

In [7], the authors presented a block based technique to detect copy-move forgery using Discrete Cosine Transform (DCT) of the image blocks. Firstly, all blocks are arranged lexicographically and then the neighboring similar pairs of blocks are regarded as copy-move region. Limitation of this method is that it fails to identify small tampered regions.

A method using Principal Component Analysis (PCA) is described in [8]. Firstly, the image is segmented into several blocks. Then their feature vectors are calculated and sorted lexicographically. The benefit of this model is that it can reduce time complexity, works good for large images. But its accuracy decreases for small sized blocks.

In [10] author proposed a detection technique for copy-move forgery based on SWT-SVD. SWT is shift invariant and noise invariant which is used to decompose the input image and helps in finding similarities between blocks of an image. This model detects image forgery for blurred image successfully.

III. Proposed Model

The purpose of proposed method is to detect copy-move forgery in digital image. First, the input image is decomposed with SWT which is later used to 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. To get the final result of matching outliers are removed. The workflow of our proposed model is shown in Figure 1.

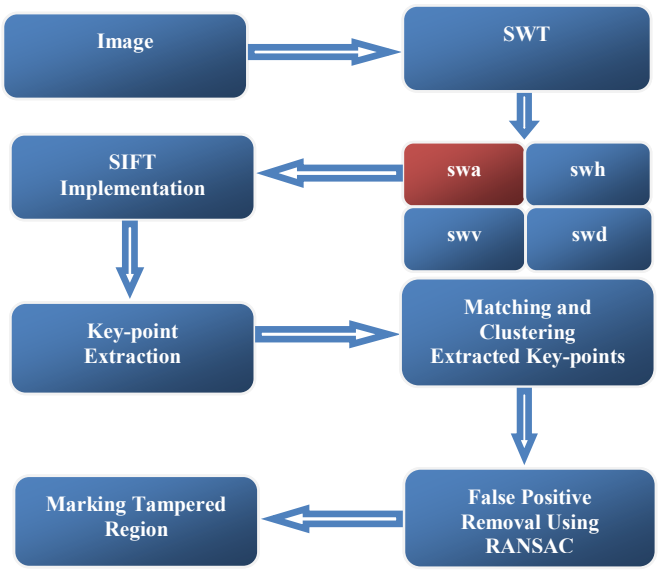

Fig. 1. Workflow of Proposed Model

A. 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.

$$IMG = 0.2989R + 0.5870G + 0.1140B \quad (1)$$

Secondly, SWT is used to obtain four sub bands such as approximate(swa),horizontal(swh),vertical(swv),diagonal(swv) .The approximate sub band is later passed as input parameter in SIFT algorithm to extract key-points features. The primary reason for choosing SWT over DCT or 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. Figure 2 shows the decomposed image by SWT on input image.

The image is divided into 4 parts in first level and in next level its swa sub-band is further decomposed [10].

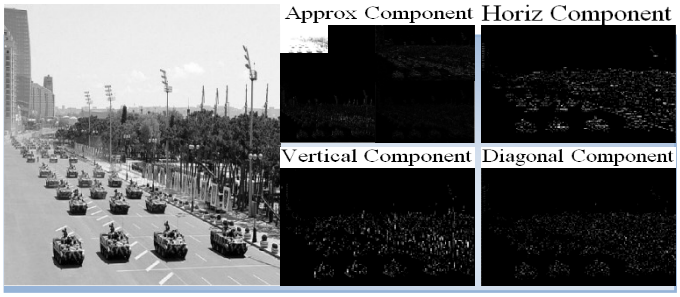

Fig. 2. 2-D SWT Decomposition of Input Image

B. SIFT Feature Extraction

SIFT is one of the best feature extracting algorithm proposed by David Lowe [11]. It is invariant to image rotation, geometrical transformation, intensity and change of viewpoint in matching features. The algorithm is divided into 4 main steps. They are as follows:

1. Scale Space Extrema Detection

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. Figure 3 shows the DoG pyramid formation of the approximate image.

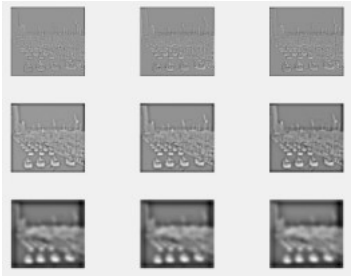

Fig. 3. DoG Pyramid Formation of Approximate Component

The key-points that are initially identified on the approximate component of decomposed image are shown in the Figure 4.

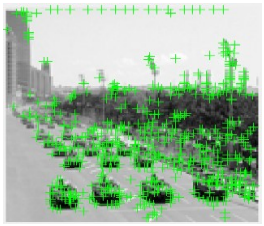

Fig. 4. Initial Location of Key-points of Different Views

2. *Key-point Localization*

In this step more accurate key-points are selected. For achieving this purpose Taylor series expansion of scale space is applied and those extrema with intensity value less than a pre-defined threshold value are rejected. The accurately selected key-points on the approximate image after discarding the ones having poor contrast are shown in Figure 5.

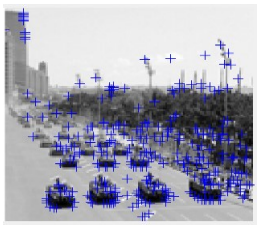

Fig. 5. Accurately Selected Key-points

3. *Assignment of Orientation*

According to the local image properties, each key-point is given an orientation. To calculate gradient direction of key-points, HOG is applied. Dominant direction of the local gradients is represented by orientation histogram peaks.

4. *Generation of Key-point Descriptors*

The measurement of the local image gradient is taken at the selected scale in the area around every key-point. Key-point descriptors use a set of 16 histograms each having 8 elements. So total no of elements in the feature vectors is 128.

C. *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.

D. *Clustering*

Agglomerative hierarchical clustering is used to group the identified matched pairs of key-points. Several Linkage methods are used to complete the clustering process. If at least two clusters having more than three matched pairs are found then the image is considered as forged.

E. *False Positive Matches Removal*

In this step we use a sorting algorithm named RANSAC [13] to remove false positive matches. In this algorithm a number of arbitrary pairs of points from the pool of matched pairs of points are selected and compared with other remaining matched pairs in terms of distance. A threshold value is set and pairs with distance within the threshold value are considered as actual matched pairs and others are rejected.

IV. Result and Discussions

We applied our model over the standard dataset MICC-F220 [12] as well as some of our own images. We have used MATLAB 2017a software with 8GB Ram and Intel core i5 processor. Firstly, 2-D SWT is applied on the dataset and approximate component of the decomposed image is passed as input parameter in SIFT algorithm to extract the descriptor vectors. Finally, matching operation is performed on the extracted key-points to detect copy-move tampering.

Figure 6 shows the original and forged image side by side and the bottom image shows the output after detection of forged region.

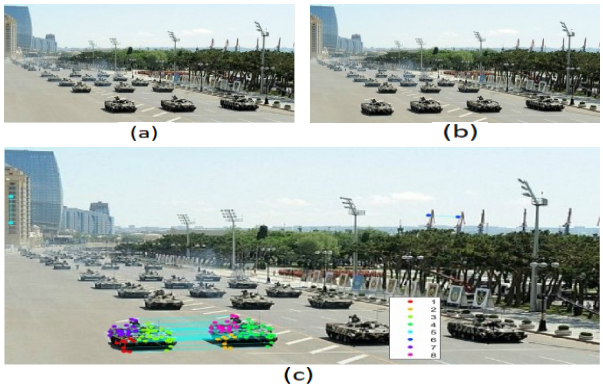

Fig. 6. (a) Original, (b) Forged, (c) Forgery Detection

We have calculated result of proposed model based on the performance analysis factors shown in Table I.

TABLE I. PERFORMANCE ANALYSIS FACTORS

Abbreviation	Full Form	Meaning
TP	True Positive	# Forged Image Detected As Forged
FP	False Positive	# Authentic Image Detected As Forged
TN	True Negative	# Authentic Image Detected As Authentic
FN	False Negative	# Forged Image Detected As Authentic

We applied the proposed model on 100 images from the dataset MICC-F220 [12]. Table II shows the result.

TABLE II. OUTCOME OF PROPOSED METHOD

No of Original Images	**No of Forged Images**	**TP**	**TN**	**FP**	**FN**
50	50	45	48	2	5

We use the following functions to measure the performance of proposed model

$$Accuracy = \frac{TP+TN}{TN+FP+TP+FN} \quad (2)$$

$$Sensitivity = \frac{TP}{TP + FN} \quad (3)$$

$$Specificity = \frac{TN}{TN + FP} \quad (4)$$

$$FPR = 1 - Specificity \text{ (FPR: False Positive Rate)} \quad (5)$$

$$FNR = 1 - Sensitivity \text{ (FNR: False Negative Rate)} \quad (6)$$

Based on the result from Table II, we show the performance of proposed model in Table III.

Table III. PERFORMANCE OF PROPOSED METHOD

Sensitivity	Specificity	Accuracy	FPR%	FNR%
90%	96%	93%	4%	10%

We compare the performance of proposed model on different types of tampering e.g. rotation, scaling, and combination of both on a certain image from the dataset. The result is shown in Table IV.

TABLE IV. PERFORMANCE ANALYSIS BASED ON DIFFERENT ATTACKS ON THE IMAGE

Types of attack	Numbers of Key-points Found	Number of Matched Key-points Detected	Computational Time (s)
No Scaling and Rotation	397	22	8. 71
Scaling	376	20	7.16
Rotation	259	13	5.49
Rotation and Scaling	287	21	7.63

Comparison among other existing models and proposed model based on true positive rate, false positive rate and average of total execution time is shown in Table V.

TABLE V: COMPARATIVE ANALYSIS WITH EXISTING MODELS

Method	FPR(%)	TRP(%)	Time(s)
Popescu and Farid [8]	86	87	70.97
Fridrich et al [7]	84	89	294.69
Proposed Method	4	90	4.83

V. CONCLUSION

This paper presents a robust key-point based copy-move forgery detection method in digital image by applying SWT decomposition technique with SIFT feature extraction algorithm. SWT is shift invariant, blur and noise invariant. With the simulation performed on original and copied images, it shows that SWT and SIFT perform better in terms of time complexity and accuracy. The combination of SWT and SIFT also shows better performance than DWT and SIFT. 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.

REFERENCES

[1] J. Li, X. Li, B. Yang and X. Sun, "Segmentation-Based Image Copy-Move Forgery Detection Scheme," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 507-518, 2015.

[2] T. Mahmood et al., "A survey on block based copy move image forgery detection techniques," *2015 International Conference on Emerging Technologies (ICET)*, Peshawar, pp. 1-6, 2015.

[3] T. K. Huynh, K. V. Huynh, T. Le-Tien and S. C. Nguyen, "A survey on Image Forgery Detection techniques," *The 2015 IEEE RIVF International Conference on Computing & Communication Technologies - Research, Innovation, and Vision for Future (RIVF)*, Can Tho, pp. 71-76, 2015.

[4] V. T. Manu and B. M. Mehtre. "Detection of copy-move forgery in images using segmentation and SURF," *Advances in Signal Processing and Intelligent Recognition Systems*, vol. 425, pp. 645-654, 2016.

[5] N. P. Joglekar and P. N. Chatur, "A Compressive Survey on Active and Passive Methods for Image Forgery Detection," *International Journal of Engineering & Computer Science*, vol. 4, no. 1, pp.10187-10190, 2015.

[6] S. Prasad and B. Ramkumar, "Passive copy-move forgery detection using SIFT, HOG and SURF features," *2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, Bangalore, pp. 706-710, 2016.

[7] J. Fridrich, D. Soukal, and J. Lukas, "Detection of copy-move forgery indigital images," in *Proceedings of the Digital Forensic Research Workshop*, 2003.

[8] A. C. Popescu and H. Farid, "Exposing Digital Forgeries By Detecting Duplicated Image Regions," Rep. TR2004-515, Dartmouth College, Computer Science, Hanover, Conn, USA, 2004.

[9] M. F. Hashmi, V. Anand and A. G. Keskar, "Copy-Move Image Forgery Detection Using an Efficient and Robust Method Combining Un-decimated Wavelet Transform and Scale Invariant Feature Transform," *Aasri Procedia*, vol. 9, pp. 84-91, 2014.

[10] R. Dixit, R. Naskar and S. Mishra, "Blur-invariant copy-move forgery detection technique with improved detection accuracy utilising SWT-SVD," *IET Image Processing*, vol. 11, no. 5, pp. 301-309, 2017.

[11] D. G. Lowe, "Distinctive Image Features from Scale-Invariant Keypoints," *International Journal of Computer Vision*, vol. 60, no. 2, pp. 91-110, 2004.

[12] 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 Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1099-1110, 2011.

[13] Y. Zhu, X. Shen and H. Chen, "Copy-Move Forgery Detection Based on Scaled ORB," *Multimedia Tools and Applications*, vol. 75, no. 6, pp. 3221-3233, 2016.