Multistage Image Cloning Detection Based on Adaptive Segmentation

Minu C M[1], Sheema Madhusudhanan[2]

[1]*MTech Cyber Security, Dept. of CSE, SNGCE, Kadayiruppu, Kerala, India.*
[2]*Asst. Prof. MTech Cyber Security, Dept. of CSE, SNGCE, Kadayiruppu, Kerala, India.*

Abstract – *In digital image manipulation the images are converted into desired image by various tools. Detection of such kind of manipulation with digital images especially the cloning is the main area of this work. Earlier the cloning detection is done by either keypoint based or block based alone. In this paper we propose an integrating Adaptive segmentation which segments image into non overlapping and irregular blocks which increases the effectiveness of segment based image Copy Move Forgery Detection. To detect cloning with more accuracy while segment feature matching we have introduced an additional stage which refines the segments according to a threshold value. This Segment refining stage will increase the accuracy and detection speed since it rejects the unwanted segments so that only valid segments are matched. The experimental results are showing the increase in efficiency and accuracy in existing methods in the proposed scheme.*

Key Words: Cloning Forgery Detection, Image forensics, Adaptive Segmentation.

1.INTRODUCTION

With increasing technical advances, computer graphics are becoming more photos realistic. Manipulation and editing of digital images are easy due to availability of powerful image processing and editing software. Detection of malicious manipulation with digital images(digital forgeries) is thus important in current era. Manipulation is performed to the visible surface can be categorized into three major groups based on the process involved in creating fake images. The groups are Retouching, Image splicing, and Copy-Move Attack. In which most of the research works are going on in Copy-Move (Cloning).

To clone or copy and paste a part of the image to conceal an object or person is one of the most commonly used image manipulation techniques. When it is done with care, it becomes almost impossible to detect the clone visually and since the cloned region can be of any shape and size and can be located anywhere in the image, it is not computationally possible to make an exhaustive search of all sizes to all possible image locations. Cloning detection methods are either keypoint-based methods or block-based methods. Most advanced methods are using segmentation based methods to detect cloning in an image. In this work we integrated adaptive segmentation to improve the segmentation. This system requires no additional computational cost as opposed to existing methods. The disadvantage in all cloning detection methods is that the detection results are not accurate enough and false positive and false negatives are high. The segmentation based techniques on the other hand avoids some false detection in traditional methods [1].

The segmentation method has the disadvantage of being less accurate in the segmenting process and segment matching and time consuming in images with different resolution. To remedy this situation adaptive segmentation which adaptively select the size by which the image segments to non over lapping patches and proposed segment refining to get more accurate and robust detection result.

2.RELATED WORK

Christlein et al [2] examined different existing CMFD method within unified workflow used under different image attributes, like different image sizes and quantities of JPEG compression. CMFD methods are either keypoint-based methods or block-based methods. They presented a common pipeline for copy-move forgery detection. In block-based methods, an image is broken up into blocks, and then a feature vector is extracted from each one. To figure out the similar area, most methods involve lexicographic sorting which recognizes similar vectors. DCT, PCA, KPCA, Zernike and DWT are some of the block based algorithms. Keypoint-based methods detects the forgery by spotting the high entropy areas, which are called the "keypoints". This method is less complex because it has fewer feature vectors involved and that means less calculations and faster process altogether. The two commonly used key-point methods used are: Scale Invariant Feature Transform (SIFT) features and Speed Up Robust Features (SURF) features.

Davide Lowe in [3] proposed SIFT algorithm to extract the features in the image and also matching the features in the same image and that way identifying the copy move forgery. Achanta et al [4] introduces an effective method for segmenting an image. In order to separate the copying source region from the pasting target region, the image should be segmented into small patches, each of which is semantically independent to the others. They introduce a new superpixel algorithm, simple linear iterative clustering (SLIC), which adapts a k-means clustering approach to efficiently generate superpixels. It is faster and more memory efficient, which improves segmentation performance. Chi-Man Pun et al [5] proposed adaptive block based segmentation method to improve the efficiency of the detection.

3. CLONING DETECTION METHOD

Of the existing types of Cloning Detection Methods that is block-based algorithms and feature keypoint-based algorithms, keypoint-based algorithms are more efficient. In the system proposed in this paper we use the SIFT features of an image when adaptive segmentation and segment refining method.

Segmentation methods are coming to this field newly where automating segmentation of the image is done before feature extraction. Of the existing segmentation based forgery schemes, the host image was usually divided into non-overlapping irregular blocks, with the region size being defined and fixed beforehand and refining matches in two stages. But the false positive rate(Original regions are detecting as forged)is comparatively higher. In this work we propose to apply the concepts of adaptive over segmentation to study its effectiveness in cloning detection. Chi-Man Pun et al [5] in their work has achieved 96% of precision and 100% of recall by using adaptive over segmentation.

Fig-1 gives the Flowchart of the proposed CMFD framework of the system. First, an adaptive segmentation method is applied to segment the input image into non-overlapping and irregular patches with the help of superpixel algorithm. Then, main keypoint features are extracted from each segment by the Scale Invariant Feature Transform (SIFT). Subsequently, the these features are matched with one another, and the feature points that are successfully matched to one another are determined to be best matched points, which can approximately indicate the suspected forgery regions. Finally, matching the segment to assure the segment detected for the forgery is correct or not by calculating and setting the threshold.

3.2 Architecture

The cloning detection method operates in multiple stages: Adaptive Segmentation, SIFT feature extraction, Matching features and Segments refining. An Adaptive Segmentation method, which is integrated into the SLIC algorithm that can calculate the regionsize from the respective image and can segment the image automatically.

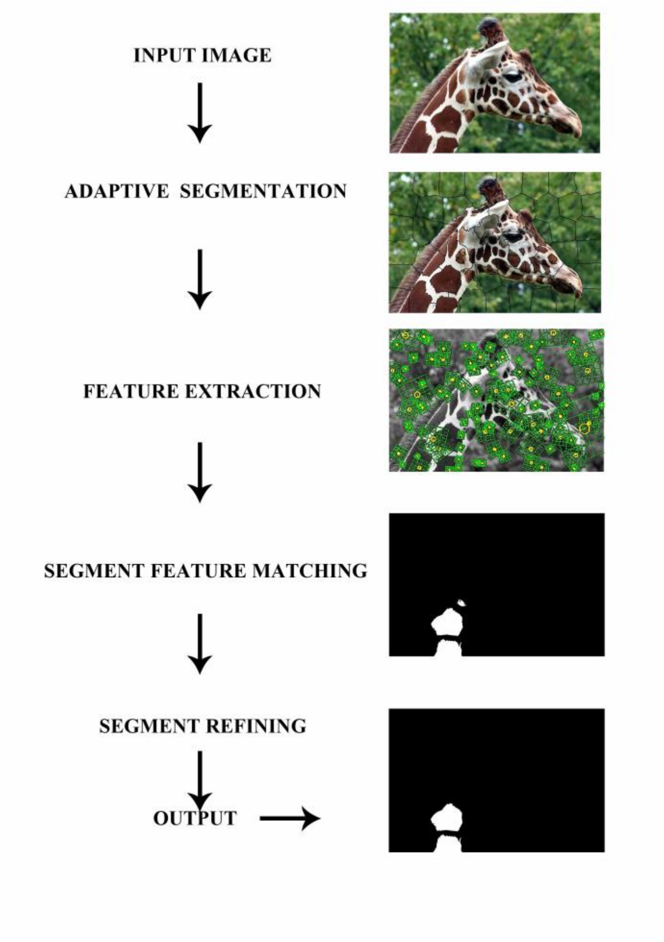

Fig -1: Flowchart of the proposed Cloning Detection method

The adaptive segmentation is done by calculated by using the Discrete Wave Transformation of the image. The Discrete Wavelet Transform (DWT) is employed to analyze the frequency distribution of the host image. In the proposed method at first a four-level DWT, using the 'Haar' wavelet, on the host image is done; then, according to Chi-Man Pun el al [5],the low-frequency energy ELF and high-frequency energy EHF can be calculated using

$$ELF = \sum |CA_4|$$

$$EHF = \sum \left(\sum |CD_i| + \sum |CH_i| + \sum |CV_i| \right), i = 1, 2, 3, 4.$$

With the low-frequency energy ELF and high frequency energy EHF , we can calculate the percentage of the low-frequency distribution PLF and according to this the regionsize S of the segment can be defined.

$$S = \begin{cases} \sqrt{0.02 * M * N}, & \text{if } PLF \geq 50\% \\ \sqrt{0.01 * M * N}, & \text{if } PLF \leq 50\% \end{cases}$$

$$PLF = \frac{ELF}{ELF + EHF}.100\%$$

Where CA4 indicates the approximation coefficients at the 4th level of DWT; and CD_i , CH_i and CV_i indicate the detailed coefficients at the i^{th} level of DWT, i= 1, 2,..., 4. where S means the initial size of the superpixels; M $*$ N indicates the size of the host image; and PLF means the percentage of the low frequency distribution. This initial size is given as regionsize of the SLIC superpixel segmentation algorithm to divide the image into non overlapping irregular patches.

Feature extraction is done by SIFT algorithm. After getting the SIFT keypoints from each segment then in the Segment Feature Matching stage, matching between each segments is done. In this matching stage we look for suspicious pairs of matches. It is done by comparing each feature with one another with the help of Euclidean Norm. With the help of THRESH, most patches are eliminated from the estimation of transform matrix.

After detecting the suspicious patches we have to determine the relationship between them. And we estimate the relationship between these two regions in terms of a transform matrix which is defined

$$\vec{x} = H\vec{x'}$$

where x and x' are the coordinates of the pixels in the copying source region and pasting target region. To find a transform matrix H RANSAC[6] is used.

Segment Refining stage is necessary because even after the second stage of matching the detection result may contains some false detection. This segment refining is integrated by a method followed from [5]. In this stage at first the correlation coefficient is calculated which indicates the number of matched feature points between the corresponding two matched segments. Then segment matching threshold is calculated. With the calculated segment refining threshold , if the correlation coefficient of the segment pair is larger than the threshold , the corresponding segment pair will be determined to be matched blocks and are labeled to indicate the suspected forgery regions.

4. RESULT AND ANALYSIS

The image dataset in [7] is used to test the proposed method. This dataset contains images with different resolutions. Fig -2 shows the host image segmentations with the proposed extended Adaptive Segmentation method and its results.

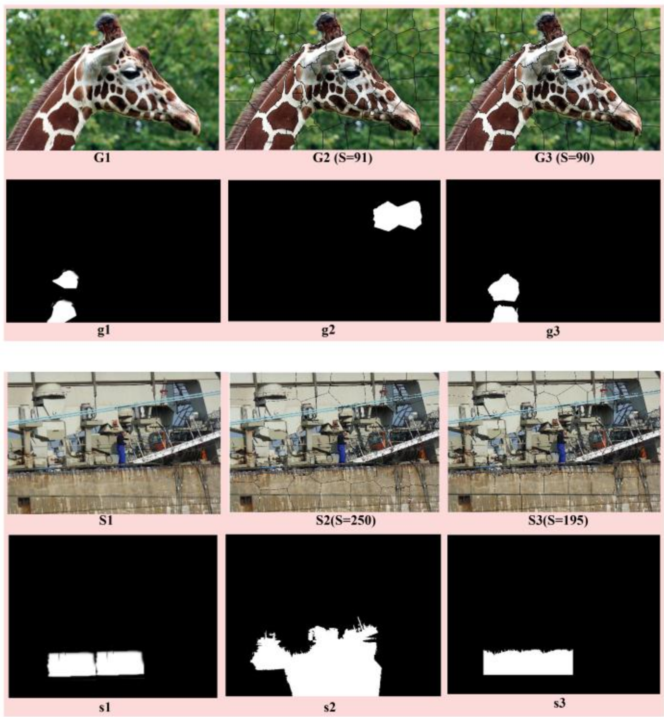

Fig -1: Different segment regionsizes and the corresponding forgery detection results

On going through series of experiments it is noticed that threshold settings is one important for getting correct detection result. Chart -1 shows the ROC curve for the trade-off between false positive and false negative when changing THRESH.

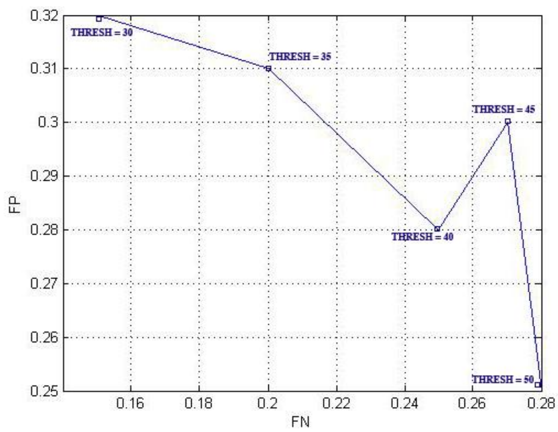

Chart -1: ROC for Threshold settings

Precision and recall is the main the two characteristics used to evaluate the performance of the proposed forgery detection scheme. In general, a higher precision and a higher recall indicate superior performance. In addition to the precision and recall, there F_1 like in score as a reference parameter to measure the forgery detection result; the F1 score combines both the precision and recall into a single value, and it can be calculated using

$$F_1 = \frac{precision * recall}{precision + recall}$$

Table–1gives the results of error measure on two systems.

Table -1: Forgery detection results of existing and proposed system

	Precision(%)		Recall(%)		F_1	
	G1	S1	G1	S1	G1	S1
EXISTING SYSTEM	93	92	98	98	95.43	94.9
PROPOSED SYSTEM	95	93	100	99.14	97.43	95.97

3. CONCLUSIONS

Images forgeries created with cloning operations are challenging to detect. The system implements Image Cloning Detection based on the segmentation and keypoint features. The concept of adaptive over segmentation is used for segmenting the image, which uses the extended version of SLIC segmentation. Both realtime forged images and database images are used in the experimental setup. Different sized images are used for checking the detection accuracy. Using this approach, for each image, we can determine an appropriate segment size to enhance the accuracy of the forgery detection results and, at the same time, reduce the computational expenses. Accuracy depends on the image size. Integration used here to increase the accuracy of the detection decreasing the false positives from .35 to .25 and false negatives from .17 to .15. Detection precision is 95% to 97%.

REFERENCES

[1] Jian Li, Xiaolong Li, Bin Yang, and Xingming Sun, "Segmentation-Based Image Copy-Move Forgery Detection Scheme" IEEE Trans. Inf. Forensics Security, VOL. 10, NO. 3, MARCH 2015.

[2] 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.

[3] D.G. Lowe, Method and apparatus for identifying scale invariant features in an image and use of same for locating an object in an image, March 23 2004, US Patent 6,711,293.

[4] R. Achanta, A. Shaji, K. Smith, A. Lucchi, P. Fua, and S. Susstrunk, "SLIC superpixels compared to state-of-the-art superpixel methods," IEEE Trans. Pattern Anal. Mach. Intell., vol. 34, no. 11, pp. 2274-2282, Nov. 2012.

[5] Chi-Man Pun, Xiao-Chen Yuan, and Xiu-Li Bi, "Image Forgery Detection Using Adaptive Over-Segmentation and Feature Point Matching" IEEE Trans. Inf. Forensics Security, VOL. 10, NO. 8, June 2015

[6] M. A. Fischler and R. C. Bolles, "Random sample consensus: A paradigm for model fitting with applications to image analysis and automated cartography," Commun. ACM.,vol. 24, no. 6, pp. 381-395, Jun. 1981.

[7] I. Amerini, L. Ballan, R. Caldelli, A. D. Bimbo, L. D. Tongo, and G. Serra, "Copy-move forgery detection and localization by means of robust clustering with J-Linkage," Signal Process., Image Commun, vol. 28, no. 6, pp. 659-669, Jul. 2013.