IMAGE FORGERY DETECTION USING ADAPTIVE OVER-SEGMENTATION AND FEATURE POINT MATCHING USING MATLAB

Dr.R. Prema	Ala. Vyshnavi	P.S.R.Ranjitha
AP/CSE	B.E(CSE)	B.E(CSE)
SCSVMV University	SCSVMV University	SCSVMV University
Kanchipuram	Kanchipuram	Kanchipuram

ABSTRACT

Digital image forgery has gotten easier to do as computer technology and image processing tools have advanced. The validity of digital images, however, is a significant problem because they are a common source of information. The adaptive over-segmentation and feature point matching approach outlined below is a recommended technique for identifying fake images using a Matlab software method. Block-based and keypoint-based forgery detection techniques are both integrated into the suggested scheme. First, the proposed Adaptive Over-Segmentation algorithm adaptively and non-overlappingly segments the host picture into irregular blocks using image processing methods. Once the feature points have been extracted from each block as block features, the block features are compared to one another to locate the labeled feature points. This process can roughly identify the regions where a forgery is believed to have taken place. To produce the identified forgery regions, it then applies the morphological operation to the merged regions. The experimental findings show that, in comparison to the current state-of-the-art copy-move forgery detection methods, the proposed copy-move forgery detection scheme can produce significantly better detection results even under a variety of difficult conditions.

KEYWORDS: Matlab, Adaptive over-segmentation, Colour block feature, Image matching

INTRODUCTION

Digital image forgery has gotten easier to do as computer technology and image processing tools have advanced. The validity of digital images, however, is a significant problem because they are a common source of information. The adaptive over-segmentation and feature point matching approach outlined below is a recommended technique for identifying fake images using a Matlab software method. Block-based and key point-based forgery detection techniques are both integrated into the suggested scheme. First, the proposed Adaptive Over-Segmentation algorithm adaptively and non-overlappingly segments the host picture into irregular blocks using image processing methods. Once the feature points have been extracted from each block as block features, the block features are compared to one another to locate the labeled feature points. This process can roughly identify the regions where a forgery is believed to have taken place. To produce the identified forgery regions, it then applies the morphological operation to the merged regions. The experimental findings show that, in comparison to the current state-of-the-art copy-move forgery detection methods, the proposed copy-move forgery detection scheme can produce significantly better detection results even under a variety of difficult conditions.

LITERATURE SURVEY

.

- Title: "Rotation Invariant Localization of Duplicated Image Regions Based on Zernike Moments".
- Authors: S. J. Ryu, M. Kirchner, M. J. Lee, and H. K. Lee.
- Publication: Ieee Transactions on Information Forensics and Security, vol. 8, pp. 1355 1370, Aug 2013. This paper proposes a forensic technique to localize duplicated image regions based on

Blocks of tiny images during Zernike moments. We take advantage of rotation invariance characteristics to accurately identify duplicated areas following any rotation. To minimize false positives, we develop a novel block-matching method based on locality-sensitive hashing. A large-scale experimental test setup compares the efficacy of our algorithm to leading techniques from several angles, looking at both pixel- and image-level detection. By considering signal characteristics and distinguishing between "textured" and "smooth" duplicated regions, especially when the duplicated regions are smooth, we find thatthe suggested method performs better than the prior art.

- Title: "Exposing Postprocessed Copy–Paste Forgeries Through Transform Invariant Features"
- Authors: P. Kakar and N. Sudha

- Publication: Information Forensics and Security, IEEE Transactions on, vol. 7, pp. 1018-1028,2012.

With increasing ease of access to powerful computing capabilities, image manipulation has become ubiquitous. The copy-paste forgery, in which a portion of an image is changed with a portion of the same image, is one of the most popular kinds of image forgeries. The problem with most previous methods for identifying identical regions is that they are unable to recognize the cloned region when it has undergone a geometric transformation. In this article, we suggest a novel method based on features that are transform-invariant. The features from the MPEG-7 image signature tools are used to acquire these.

EXISTING SYSTEM

In the existing types of image tampering, a common manipulation of a digital image is a copy-move forgery, which is to paste one or several copied regions (S) of an image into other parts of the same image. In previous years, many forgery detection methods have been proposed for copy-move forgery detection. According to the existing methods, the copy–move forgery detection methods can be categorized into two main categories: block-based algorithms and feature key point–based algorithms. The existing block-based forgery detection methods divide the input images into overlapping and regular image blocks; then, the tampered region can be obtained by matching blocks of image pixels or transform coefficients.

PROBLEM STATEMENT

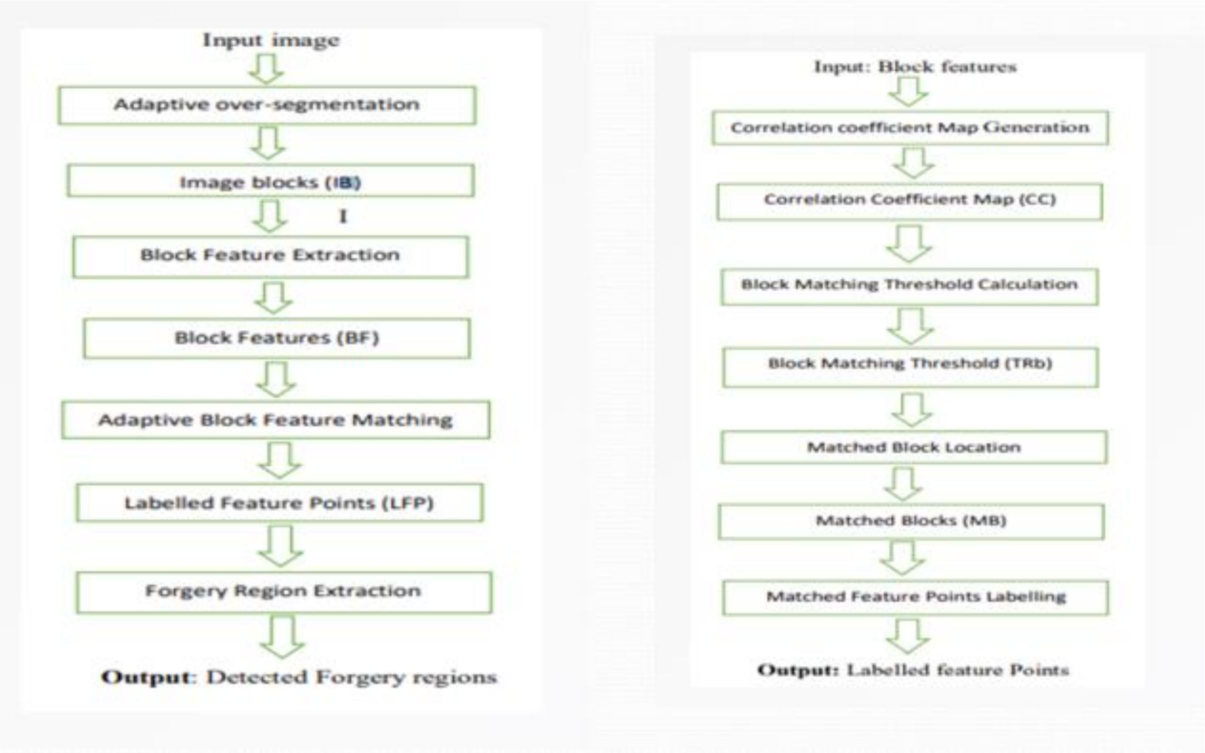
Most of the existing block–based forgery detection algorithms use a similar framework, and the only difference is that they apply different feature extraction methods to extract the block features. Digital images are a popular source of information, and the reliability of digital images is becoming an important issue. To detect the forgery regions more accurately, we propose the Forgery Region Extraction algorithm, which replaces the feature points with small superpixels as feature blocks and merges the neighboring blocks that have similar local color feature blocks to generate the merged regions.

PROPOSED SYSTEM

This section describes the proposed image forgery detection using adaptive over-segmentation and feature point matching in detail. Fig. 1 shows the framework of the proposed image forgery detection scheme.

First, an adaptive over-segmentation method is proposed to segment the host image into non-overlapping and irregular blocks called Image Blocks (IB). Then, we apply the Scale Invariant Feature Transform (SIFT) in each block to extract the SIFT feature points as Block Features (BF). Subsequently, the block features are matched with one another, and the feature points that are successfully matched to one another are determined to be Labeled Feature Points (LFP), which can approximately indicate the suspected forgery regions. Finally, we propose the Forgery Region Extraction method to detect the forgery region from the host image according to the extracted LFP.

ARCHITECTURE


Input image
Adaptive over-segmentation
Image blocks (IB)
I
Block Feature Extraction
Block Features (BF)
Adaptive Block Feature Matching
Labelled Feature Points (LFP)
Forgery Region Extraction
Output: Detected Forgery regions
Input: Block features
Correlation coefficient Map Generation
Correlation Coefficient Map (CC)
Block Matching Threshold Calculation
Block Matching Threshold (TRb)
Matched Block Location
Matched Blocks (MB)
Matched Feature Points Labelling
Output: Labelled feature Points

ALGORITHM

ADAPTIVE OVER-SEGMENTATION ALGORITHM:

Block-based forgery detection methods can divide the host image into blocks.

• The host image was usually divided into overlapping regular blocks,.

• Then, the forgery regions were detected by matching those blocks. In this way, the detected regions are always composed of regular blocks.

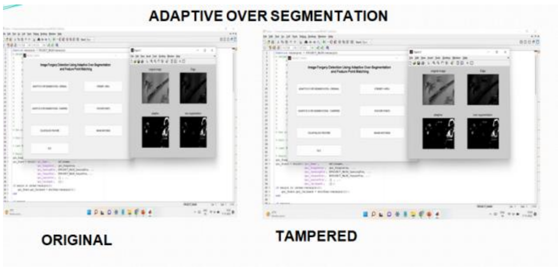
BLOCK FEATURE ALGORITHM:

• Extract feature points from each image block as block features, and the feature points should be robust to various distortions.

• copy-move pairs are identified by searching blocks with similar features.

• High similarity between feature vectors can be interpreted as duplicated regions.

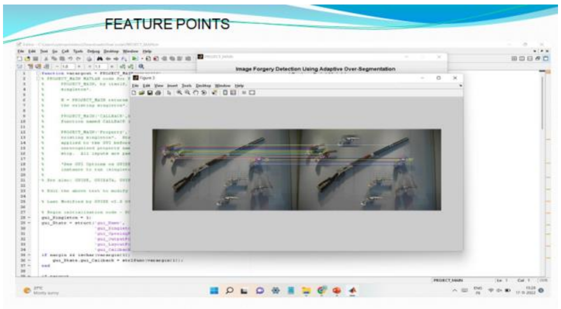
EXPERIMENTAL ANALYSIS



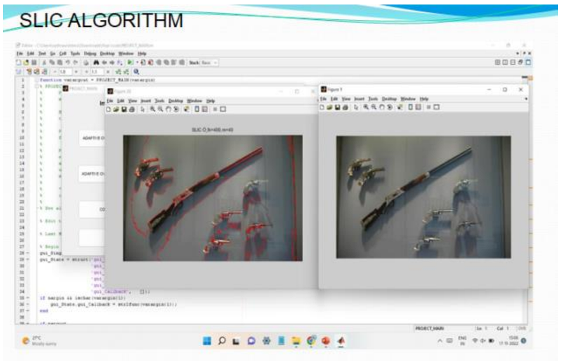
ADAPTIVE OVER SEGMENTATION

ORIGINAL

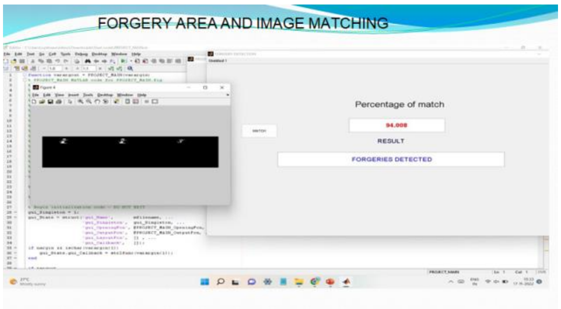
TAMPERED



FEATURE POINTS



SLIC ALGORITHM



FORGERY AREA AND IMAGE MATCHING

Percentage of match

94.008

RESULT

FORGERIES DETECTED

CONCLUSION

Using the aforementioned review articles from IEEE Paper, we have reached this conclusion regarding forgery detection. It can be difficult to spot digital forgery images produced using copy-move processes. In this article, we present an innovative copy-move forgery detection method based on feature point matching and adaptive over-segmentation. According to the provided host images, the adaptive over-segmentation algorithm is proposed to segment the hostimage into non-overlapping and irregular blocks. Using this method, we can choose an appropriate block initial size for each image to improve the accuracy of the forgery detection results while at the same time lowering the computational costs. Then, the feature points are extracted from each block as block features, and the Block Feature Matching algorithm is suggested. This method locates the labeled feature points by matching block features with one another; the process can roughly identify the regions that may be forgery suspects. Then, to identify the more precise forgery regions, we suggest the Forgery Region Extraction algorithm, in which the labeled feature points are changed to small super pixels to serve as feature blocks, and the nearby feature blocks with related local color features are combined to produce the merged regions. The merged regions are then subjected to morphological operation to produce the forgery regions that have been identified. With a large number of experiments, we show howsuccessful the suggested plan is. In comparison to the current state-of-the-art copy-move forgerydetection schemes, experimental findings demonstrate that the proposed scheme can detect copy-move forgery images under a variety of difficult conditions, including geometric transforms, JPEG compression, and down-sampling. Future research might concentrate on applying the suggested adaptive over-segmentation and feature point matching forgery detection method to other types of forgery,

like splicing, or other types of media. Like video and audio.

REFERENCES

[1] A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, "Detection of copy-move forgery in digital images," in Proceedings of Digital Forensic Research Workshop, 2003

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

[3] W. Luo, J. Huang, and G. Qiu, "Robust detection of region-duplication forgery in the digital

image," in Pattern Recognition, 2006. ICPR 2006. 18th International Conference on, 2006, pp.746-749.

[4] G. Li, Q. Wu, D. Tu, and S. Sun, "A sorted neighborhood approach for detecting duplicatedregions in image forgeries based on DWT and SVD," in Multimedia and Expo, 2007 IEEE International Conference on, 2007, pp. 1750-1753.

[5] B. Mahdian and S. Saic, "Detection of copy–move forgery using a method based on blur moment invariants," Forensic science international, vol. 171, pp. 180-189, 2007.

[6] X. Kang and S. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics," in Computer Science and Software Engineering, 2008 International Conference on, 2008, pp. 926-930.

[7] S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on, 2009, pp. 1053-1056.

[8] J. Wang, G. Liu, H. Li, Y. Dai, and Z. Wang, "Detection of image region duplication forgery using a model with circle block," in Multimedia Information Networking and Security, 2009. MINES'09. International Conference on, 2009, pp. 25-29.

[9] J. Wang, G. Liu, Z. Zhang, Y. Dai, and Z. Wang, "Fast and robust forensics for image region-duplication forgery," Acta Automatica Sinica, vol. 35, pp. 1488-1495, 2009.

[10] H. Lin, C. Wang, and Y. Kao, "Fast copy-move forgery detection," WSEAS Transactions on Signal Processing, vol. 5, pp. 188-197, 2009.

[11] S. Ryu, M. Lee, and H. Lee, "Detection of copy-rotate-move forgery using Zernike moments," in Information Hiding, 2010, pp. 51-65.

[12] S. J. Ryu, M. Kirchner, M. J. Lee, and H. K. Lee, "Rotation Invariant Localization of Duplicated Image Regions Based on Zernike Moments," Ieee Transactions on Information Forensics and Security, vol. 8, pp. 1355-1370, Aug 2013.