isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 4, Issue: 3,Special Issue: 2 ,Apr,2016 ,ISSN_NO: 2321-3337

COPY MOVE FORGERY IMAGE DETECTION

S.Saravana Kumar [1],R.Barath [2] ,Mrs.A.G.Jessy Nirmal[3]

Student, Department of Computer Science and Engineering,Agni College of Technology, India[1, 2].

Assistant Professor, Department of Computer Science and Engineering, Agni College of Technology, India [3].

ABSTRACT

We propose a method copy-move image forgery detection using feature point extraction and morphological operations. The proposed scheme integrates both block-based and key point-based forgery detection methods. First, segments the host image into non-overlapping and irregular blocks adaptively. Then, the feature points are extracted from each block as block features, and the block features are matched with one another to locate the labeled feature points; this procedure can approximately indicate the suspected forgery regions. To detect the forgery regions more accurately, And then merges the neighboring blocks that have similar local color features into the feature blocks to generate the merged regions; finally, it applies the morphological operation to the merged regions to generate the detected forgery regions. The experimental results indicate that the proposed copy-move forgery detection scheme can achieve much better detection results even under various challenging conditions.

1. INTRODUCTION

The development of computer technology and image processing software, digital image forgery has been becoming increasingly easy to perform. However, digital images are a popular source of information, and the reliability of digital images is thus becoming an important issue. Of the existing kinds of image forgery, a common manipulation with digital image is copy-move forgery, which is to paste one or several copied region(s) of an image into another part(s) of the same image. In the past years, lots of forgery detection methods have been proposed for copy-move forgery detection. To adaptively segment the host image into non-overlapping and irregular blocks. Then the feature points are extracted from each block and matched with each other to locate the labeled feature points which can approximately indicate the suspected forgery regions. Finally the labeled feature points are processed and the morphological operation is applied to generate the detected forgery regions.

2. EXISTING SYSTEM

The existing block-based forgery detection methods divide the input images into overlapping and regular image blocks; then, and then obtain the tampered regions by matching blocks of image pixels or transform coefficients; and the keypoint-based forgery detection methods, which extract the image keypoints and match them to identify the duplicated regions. In this forgery detection method in which the input image was divided into over-lapping rectangular blocks, from which the quantized Discrete Cosine Transform (DCT) coefficients of the blocks were matched to find the tampered regions. An applied Principal Component Analysis (PCA) to reduce the feature dimensions. In Used the RGB color components and direction information as block features. In Used Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) to extract the image features. In existing systems they have some limitations, although these schemes are effective in forgery detection. The host image is divided into over-lapping rectangular blocks, which would be computationally expensive as the size of the image increases. The methods cannot address significant geometrical transformations of the forgery regions. Their recall rate is low because their blocking method is a regular shape.

3. PROPOSED SYSTEM

This is proposed to segment the host image into non-overlapping and irregular blocks. Then the feature points are extracted from each block and matched with each other to locate the labeled feature points which can approximately indicate the suspected forgery regions. Finally the labeled feature points are processed and the morphological operation is applied to generate the detected forgery regions.

4. SYSTEM IMPLEMENTATION

4.1 Segmentation and Feature point detection

An adaptive over-segmentation method is proposed to segment the host image into non-overlapping and irregular blocks called Image Blocks (IB). Then, 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.

4.2 Feature Detection

In computer vision and image processing the concept of feature detection refers to methods that aim at computing abstractions of image information and making local decisions at every image point whether there is an image feature of a given type at that point or not. The resulting features will be subsets of the image domain, often in the form of isolated points, continuous curves or connected regions.

4.3 Feature extraction

Once features have been detected, a local image patch around the feature can be extracted. This extraction may involve quite considerable amounts of image processing. The result is known as a feature descriptor or feature vector. Among the approaches that are used to feature description, one can mention N-jets and local histograms (see scale-invariant feature transform for one example of a local histogram descriptor). In addition to such attribute information, the feature detection step by itself may also provide complementary attributes, such as the edge orientation and gradient magnitude in edge detection and the polarity and the strength of the blob in blob detection.

4.4 Block Feature Extraction Algorithm

Extract block features from the image blocks (IB). The traditional block-based forgery detection methods extracted features of the same length as the block features or directly used the pixels of the image block as the block features; however, those features mainly reflect the content of the image blocks, leaving out the location information. In addition, the features are not resistant to various image transformations. Therefore, we extract feature points from each image block as block features, and the feature points should be robust to various distortions, such as image scaling, rotation, and JPEG compression.

4.5 Block Feature Matching Algorithm

After we have obtained the block features (BF), we must locate the matched blocks through the block features. In most of the existing block-based methods, the block matching process outputs a specific block pair only if there are many other matching pairs in the same mutual position, assuming that they have the same shift vector. When the shift vector exceeds a user-specified threshold, the matched blocks that contributed to that specific shift vector are identified as regions that might have been copied and moved. In our algorithm, because the block feature is composed of a set of feature points, we proposed a different method to locate the matched blocks. First, the number of matched feature points is calculated, and the correlation coefficient map is generated; then, the corresponding block matching threshold is calculated adaptively; with the result, the matched block pairs are located; and finally, the matched feature points in the matched block pairs are extracted and labeled to locate the position of the suspected forgery region.

5. ARCHITECTURE DIAGRAM

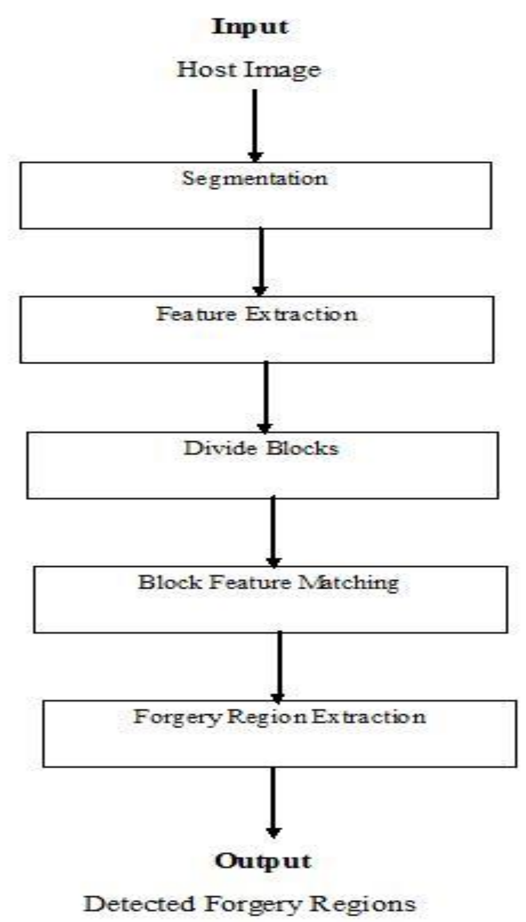

Figure 1: Architecture Diagram.

The purpose of the architecture diagram is to represent the type of software architecture that is used by the system, to describe the various hardware and software components that are used for the system implementation.

6. CONCLUSIONS

The copy move forgery detection scheme using feature point extraction and morphological operations. It can segment the host image into non-overlapping and irregular blocks. In each block, the feature points are extracted and matched to indicate the suspected forgery regions. The Forgery Region Extraction algorithm is proposed to process the suspected feature points, thus generating the detected forgery regions. Experimental results show that the proposed scheme can achieve good performance under various challenging conditions such geometric transforms, and JPEG compression.

7. FUTURE ENHANCEMENTS

Future work may focus on applying the proposed algorithm feature extraction and morphological operations are used into other kind of forgery such as splicing or other kind of media such as video and audio. Another future direction is to embed the forgery detection method with some watermarking algorithms for possible improvement in multimedia security.

8. REFERENCES

[1] “Segmentation-Based Image Copy-Move Forgery Detection Scheme” Jian Li; Xiaolong Li; Bin Yang; Xingming Sun Information Forensics and Security, IEEE Transactions onYear: 2015.

[2] “Copy move forgery detection using DWT and SIFT features” Hashmi, M.F.; Hambarde, A.R.; Keskar, A.G.Intelligent Systems Design and Applications (ISDA), 2013 13th International Conference on Year: 2013

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

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

[5] W. Luo, J. Huang, and G. Qiu, "Robust detection of region-duplication forgery in digital image," in *Pattern Recognition, 2006. ICPR 2006. 18th International Conference on*, 2006, pp. 746-749.

[6] 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.

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

[8] 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.