THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

A Passive Technique for Image Forgery Detection in Digital Images

Vaishnavee S.
Assistant Professor (CSE), Sri Krishna College of Technology, Anna University, Coimbatore, India
Kalpana P.
Assistant Professor (CSE), Sri Krishna College of Technology, Anna University, Coimbatore, India

Abstract:
Digital images are simple to operate and edit due to accessibility of much software. It is feasible to insert or eliminate some features from an image. Cloning is one of the image tampering methods, replicating the same region of the image. The proposed method works in finding the cloned and uncloned forgeries of newly added region to the real image wherein a region from an image is replaced with another region from the different image. The existing techniques in finding alike regions suffer from their lack of ability to spot the cloned region when it has been subjected to a geometric transformation. The Proposed method clearly employ the distortion cues can identify the forgery region in distortion image. Two bottom-up cues are proposed based on distortion constraint are provide to differentiate the validation of the line in the image. Then a fake saliency map is used to maximum fake detection density, and based on the fake saliency map, an energy function is provided to get the pixel-level forgery object.

Keywords: *Copy-move forgery, Distance cue, Distortion, Image forensics, Saliency map, Volume cue*

1. Introduction

The Digital image forensics concerned with multimedia security. There are many approaches for tampering detection. Generally, these approaches could be divided into active and passive blind approaches. The active methods can be divided into the watermarking (data hiding) approach and the digital signature approach. The blind methods are mainly based on verify the integrity of digital images and detect the traces of tampering without using any pre–embedded information. Nowadays passive approaches gained its value in the digital era. The availability of powerful digital image processing software, such as Photoshop, makes it relatively easy to create digital forgeries from one or multiple images. An example of a digital forgery is shown in Figure 1. The picture below shows a sample image that has been tampered using copy-move attack (left) and its original (right).

The drawback of active approach is that a watermark must be inserted at the time of recording, which would limit this approach to specially equipped digital cameras. But, passive techniques do not need any watermark or signature. These techniques work on the assumption that although digital forgeries may leave no visual clues that indicate tampering, they may alter the underlying statistics of an image.

Original image (left) and Forged image (right).
Figure 1: Example of a digital forgery

The aim of blind image forensics is to find the forgeries in digital images without using an embedded security scheme [1]. Today, copy-move forgery detection is the most actively investigated topic. Copy-move is one of the image manipulation techniques, in which a part of the image is copied and pasted in another part of the image. The main reasons for copy-move forgery are either to hide an element in the image, or to enlighten particular objects. A copy-move forgery is an easy to create. Both the source and the target regions may be from the same image, so properties like the colour temperature, illumination conditions and noise are matched well between the tampered region and the image.

In the earlier period , the area of forgery detection has emerge to validate digital images using different constraint [1]: i) pixel-based techniques [3] that have been projected to detect cloned, spliced images; ii) format-based techniques [4], [5] that identify tampering in lossy image compression; iii) camera-based techniques [6]–[7] that use artifacts introduce by the camera lens, sensor or on-chip post processing; iv) physically based techniques [8], [9] that find tampers in the image using physical rules; and v) geometric- based techniques [10], that use geometric constraints which are improved from perspective views. The proposed method based on fifth category, i.e., geometric techniques

The rest of this paper is organized as follows. In Section II, we discuss the existing work concerning the detection of image forgeries. In Section III, we discuss our proposed method and discussion in Section IV.

2. Existing System

The copy–move forgeries include covering one part of an image by overlaying another region from the same or different image. The most apparent way of finding copied and pasted regions in the image would be to validate small cluster or block of pixels for match in the image. Yet, there are two important issues with this. Firstly, this could be a computationally rigorous method, as similar blocks (or other shapes) of pixels would become impossible with large size of the image. Secondly, such a method could not succeed in case of small changes such as addition of noise. In order to get out of these drawbacks of this direct approach, researchers have developed different techniques which can be classified into two main categories: block-based and feature-based.

2.1. Block-Based Techniques

Some techniques use representation for dimensionality reduction [11], [12] such as principal component analysis (PCA) or frequency representation [13] such as discrete cosine transform (DCT) in order to powerfully find identical regions. Still, they guess that the tampered region has not undergone any post-processing. On the other hand, these techniques are invariant to small noise addition. The effort of [14] discusses enhanced vigour using DCT to noise addition, blurring and lossy compression, but does not pact with geometrical transformations of the tampered region. The technique of [15] reduces the time complexity of the PCA-based approach by means of a discrete wavelet transform (DWT), but this method does not deal geometrical transformations. In [16], the authors suggest using a set of moment invariants, PCA and a kd-tree that capably identify tampered regions. In [17] log-polar block descriptors to identify reflected, rotated and scaled regions. But, this method is vulnerable to noise addition and compression because it uses the pixels directly. The author of [18] uses Zernike moments of blocks to identify cloned forgeries with feasible rotation, but does not deal with scaling, and presents results only on a little number of forgeries produced with rigorous constraints. The authors of [19] projected a technique based on the Fourier-Mellin Transform which is invariant to resizing of the copied regions. On the other hand, this technique not comes up to scratch when the rotation or resizing is large. This technique was improved upon in [20] where major rotation invariance was achieved by taking projection along angular directions. But, the scale invariance seems to be suitable only over a small range, and the number of false positives is fairly high.

2.2. Feature-Based Techniques

Block-based techniques basically match blocks in a competent manner and present invariance to some transformations during a suitable selection of the method of representation. It is seen, however, that this often results in major false positives, and invariance to other transformations like flipping, brightness changes and blurring is tough to found. Therefore, recently, awareness in feature-based methods has been spurred, as forgeries have become more credible with a number of transformations being engaged. Feature-based techniques try to avoid these inconveniences by choosing to match image features, instead of blocks. By a proper selection of features, invariance to a number of transformations can be recognized. The motivation for this lies in the truth that the features of interest were developed for the purpose of object recognition and/or content-based image recovery and so needed to be invariant to a huge number of transformations. Our proposed method is an example of copy–move forgery detection techniques as well. The authors of [21]– [24] proposed techniques to handle various transformations using scale-invariant feature transform (SIFT) features, which are widely used in the field of computer vision. These features are, however, not vigorous to many post processing operations such as blurring, flipping and fails to detect multiple clones.

The distortion in the image provides a very essential geometric constraint, that the straight line in space is projected into a great circle on the projection sphere [25], [26]. In this paper two bottom-up cues based on this geometric constrain are introduced and use them to judge the untrustworthy likelihoods of the candidate lines.

2.3. Overview of Proposed Scheme

The digital image is given as the input for the system.

1. Extract the features of the given image (Examines every pixel to see if there is a feature present at that pixel.)
2. Two bottom-up cues based on distortion constraint are defined to measure forged region (volume cue and distance cue)
3. Saliency map estimation (is generated by the untrustworthy likelihood to express the location of forgery object)
4. Segment the forged region from the image.

3. Proposed System

A forgery recognition method based on distortion is proposed. Firstly, the untrustworthy likelihood of each candidate line is computed, by measuring the distortion cues. Then a fake saliency map is generated to convey the position of the forged region.

The main contributions of this paper are as follows.

1. Radial distortion projection (RDP) model is adopted to reduce to bare bones of the conventional captured ray-based models.
2. Geometric constraint of line in the RDP model is offered. Two bottom-up cues based on distortion constraint, the volume cue and the distance cue, are definite to measure untrustworthy likelihood of the candidate line.
3. Fake saliency maps via the untrustworthy likelihood are engaged to maximum fake saliency density and identify the forgery object. The fake saliency map could be broadly used in other forensic methods.

3.1. Feature Extraction

The input image is generally smoothed by a Gaussian kernel in a scale-space representation and more image features are computed, frequently expressed in terms of local derivative operations. The N points with the maximum responses (issue to meeting exclusion zone criteria) are considered. An exclusion zone of M pixel is used about each feature to preserve a least spatial distance between two features. This is significant because it is pretty likely that point showing the highest reaction to the filters lean to come from the same regions, and to avoid clustering of features in certain areas of the image.

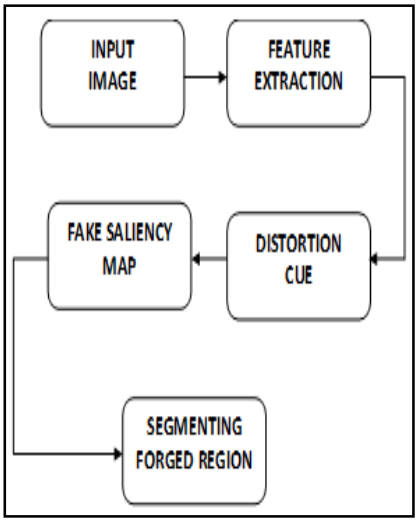

Figure 2: Proposed Technique

3.2. Distortion Cue

Two bottom-up cues based on distortion constraint are defined to measure forged region (volume cue and distance cue) With the geometrical constraint, if three points on the image plane are projected from the straight world line, their back-projected points follow the geometrical constraint where volume cue is the volume of tetrahedron made up by the center portion. Statistically, the forgery line is highly unlikely to assure this geometrical constraint. So the volume cue is one of a bottom-up cue where the length of the forgery line in the image is the curves of the volume cue of each candidate line. The volume cues of original lines are close to zero and the cues of forgery lines are more likely to be away from the zero.

The Distance cue is same as the volume cue, the distance between the center and the plane, which is defined by three projected points on the image, is also considered as a cue. If the matrix is composed of a common point and three points on the image which define the plane.

3.3. Saliency Map

The different visual features that contribute to attentive selection of a stimulus (color, orientation, movement etc) are combined into one single topographically oriented map, the Saliency map which integrates the normalized information from the individual feature maps into one global measure of conspicuity.

3.4. Segmentation

Segmentation of forgery regions in an image is a tough problem, as the forged region may noisy and incomplete. Saliency map is created by the untrustworthy likelihood to express forged region. Finally, the forgery region is segmented.

4. Experimental Results

The forgery object (region) could be located and segmented using saliency map. The saliency map is generated based on forged seed and for wrapping the region, a sequence of operations is used as described.

Some background near the forged region also has a high saliency weight. When the appearance of them is alike and the complex background and weak boundary, some details of the forgery object could not be segmented accurately. The sample of this case, where the detected region involves the original parts. The main part of the forged region is extracted by this method.

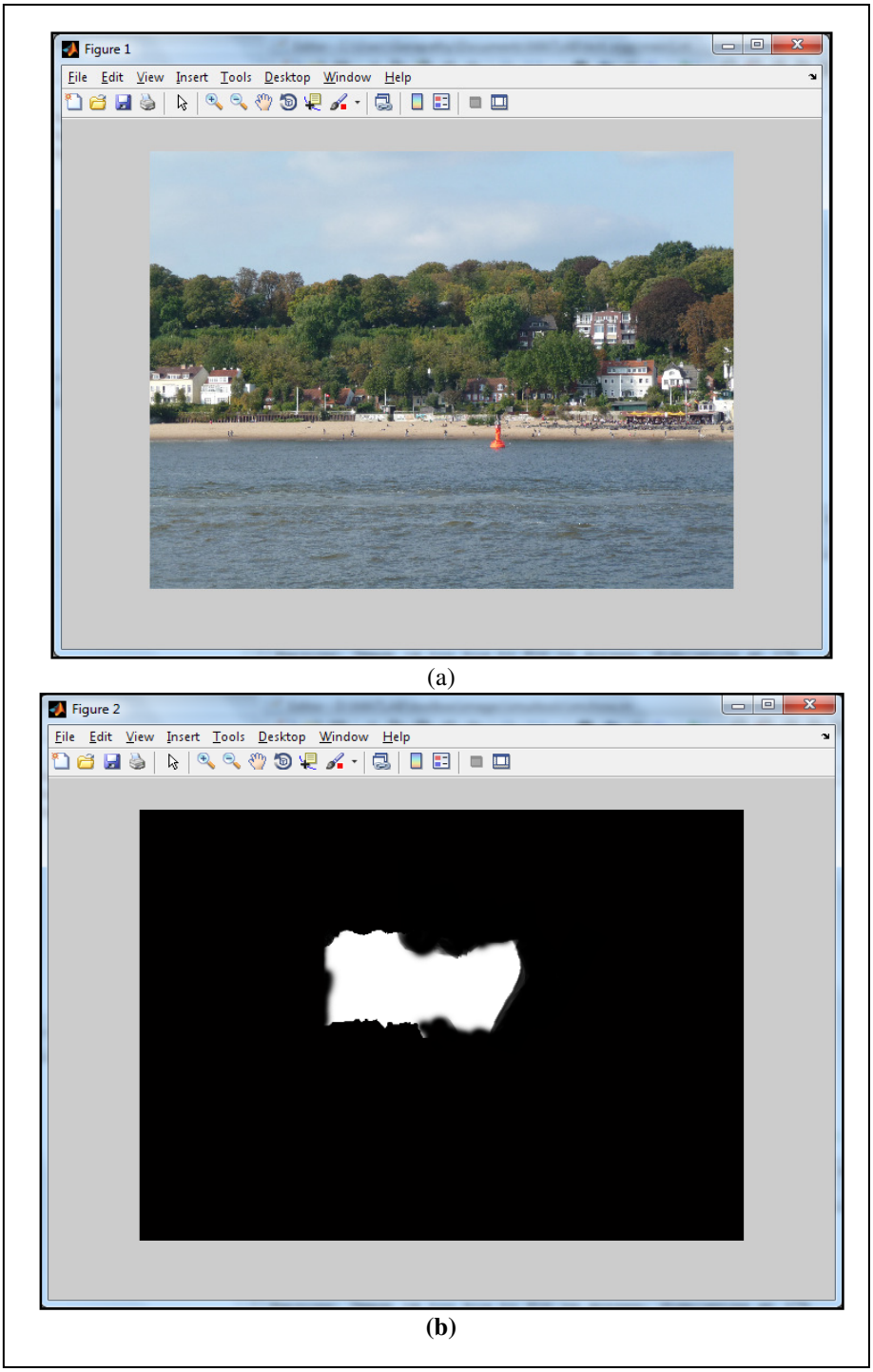

Figure 3: Tamper Detection. (a) Input Image. (b) Saliency Map.

5. Conclusion

This paper mainly aims to detect forged region in images. Image forgeries are most common method of forgery where parts of an image are replaced with other parts from the same image or other. The copied and pasted regions may be subjected to various image transformations in order to cover the tampering. Conventional techniques of detecting copy-paste forgeries have problems of false positives and vulnerability to many image processing operations. A geometric-based method is proposed for finding a forged region via distortion. The geometry constraint on the viewing changes of radial distortion projection model is employed to support two bottom-up cues. Then a saliency map is generated by untrustworthy likelihood, to detect the forgery object. The results of the preliminary testing showed a desirable consistency with those obtained from the proposed scheme. We expect this approach to detect multiple cloned forgeries.

6. References

i. H. Farid, "Asurvey of image forgery detection," IEEE Signal Process. Mag., vol. 2, no. 26, pp. 16–25, 2009.

ii. B. Mahdian and S. Saic, "A bibliography on blind methods for identifying image forgery," Image Commun., vol. 25, no. 6, pp. 389–399, 2010.

iii. A. Popescu and H. Farid, "Exposing digital forgeries by detecting traces of re-sampling," IEEE Trans. Signal Process., vol. 53, no. 2, pp. 758–767, Feb. 2005.

iv. Z. Fan and R. L. de Queiroz, "Identification of bitmap compression history: JPEG detection and quantizer estimation," IEEE Trans. ImageProcess., vol. 12, no. 2, pp. 230–235, Feb. 2003.

v. W. Luo, J. Huang, and G. Qiu, "JPEG error analysis and its applications to digital image forensics," IEEE Trans. Inf. Forensics Security, vol. 5,no. 3, pp. 480–491, Jun. 2010.

vi. M. Johnson and H. Farid, "Exposing digital forgeries through chromatic aberration," in Proc. 8th ACM Workshop Multimedia and Security, 2006, pp. 48–55.

vii. A. Swaminathan, M. Wu, and K. Liu, "Digital image forensics via intrinsic fingerprints," IEEE Trans. Inf. Forensics Security, vol. 3, no. 1, pp. 101–117, Feb. 2008.

viii. M. Johnson and H. Farid, "Exposing digital forgeries in complex lighting environments," IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 450–461, Jun. 2007.

ix. Q. Liu, X. Cao, C. Deng, and X. Guo, "Identifying image composites through shadow matte consistency," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 1111–1122, Jun. 2011.

x. W. Zhang, X. Cao, Y. Qu, Y. Hou, H. Zhao, and C. Zhang, "Detecting and extracting the photo composites using planar homography and graph cut," IEEE Trans. Inf. Forensics Security, vol. 5, no. 3, pp. 544–555, Jun. 2010.

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

xii. H. Lin, C. Wang, and Y. Kao, "Fast copy-move forgery detection," WSEAS Trans. Signal Process., vol. 5, no. 5, pp. 188–197, 2009.

xiii. J. Fridrich, B. Soukal, and A. Lukáš, "Detection of copy-move forgery in digital images," in Proc. Digital Forensic Res. Workshop, 2003.

xiv. Y. Huang,W. Lu,W. Sun, and D. Long, "Improved DCT-based detection of copy-move forgery in images," Forensic Sci. Int., vol. 206, no. 1–3, pp. 178–184, 2011.

xv. S. Khan and A. Kulkarni, "Reduced time complexity for detection of copy-move forgery using discrete wavelet transform," Int. J. Computer Applic. IJCA, vol. 6, no. 7, pp. 31–36, 2010.

xvi. B. Mahdian and S. Saic, "Detection of copy-move forgery using a method based on blur moment invariants," Forensic Sci. Int., vol. 171, no. 27–3, pp. 180–189, 2007.

xvii. S. Bravo-Solorio and A. Nandi, "Passive forensic method for detecting duplicated regions affected by reflection, rotation and scaling," in Proc. Eur. Signal Processing Conf., 2009, pp. 824–828.

xviii. S. Ryu, M. Lee, and H. Lee, "Detection of copy-rotate-move forgery using zernike moments," in Proc. Int. Workshop Information Hiding, 2010, pp. 51–65, Springer.

xix. S.Bayram, H. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in Proc. IEEE Int. Conf. Acoustics, Speech Signal Processing, 2009, pp. 1053–1056.

xx. W. Li and N. Yu, "Rotation robust detection of copy-move forgery," in Proc. IEEE Int. Conf. Image Processing, 2010, pp. 2113–2116.

xxi. H. Huang, W. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm," in Proc. IEEE Pacific-Asia Workshop Computational Intelligence Industrial Applic., 2008, pp. 272–276.

xxii. X. Pan and S. Lyu, "Region duplication detection using image feature matching," IEEE Trans. Inform. Forensics Security, vol. 5, no. 4, pp. 857–867, Aug. 2010.

xxiii. I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "ASIFT-based forensic method for copy-move attack detection and transformation recovery," IEEE Trans. Inform. Forensics Security, vol. 6, no. 3, pp. 1099–1110, Jun. 2011.

xxiv. Pravin Kakar, and N. Sudha," Exposing Post processed Copy–Paste Forgeries Through Transform-Invariant Features ", IEEE Trans. on Information forensics and Security, Vol. 7, no. 3, June 2012.

xxv. X. Ying and Z. Hu, "Catadioptric camera calibration using geometric invariants," IEEE Trans. Pattern Anal. Mach. Intell., vol. 26, no. 10, pp. 1260–1271, Oct. 2004.

xxvi. X. Ying, Z. Hu, and H. Zha, "Fisheye lenses calibration using straight line spherical perspective projection constraint," in ACCV, 2006, pp.61–70.