International Journal of Recent Trends in Engineering & Research
ISSN(ONLINE) : 2455-1457
IMPACT FACTOR : 3.344

A Survey on Copy-Move Image Forgery Detection

Miss Sonali Navale
Department of E&TC, G. E. S. R. H. Sapat College of Engineering, Nashik

Abstract—Due to rapid advances and availabilities of powerful image processing software's, it is easy to manipulate and modify digital images. So it is very difficult for a viewer to judge the authenticity of a given image.For digital photographs to be used as evidence in law issues or to be circulated in mass media, it is necessary to check the authenticity of the image. So In this paper, describes various methods for an Image forgery detection.

Keywords—Image tampering, geometric transformation, image forensics, authenticity.

I. INTRODUCTION

Images have acquired the reputation of being inarguable evidence. However, with the development of imaging technology and the accessibility of powerful affordable image editing tools like Photoshop, the evidence of tampering on digital images is extremely difficult to uncover. As a result, today digital images are losing authenticity and taking their authenticity for granted is becoming increasingly difficult in legal cases, in electronic media, in medical profession, and in financial institutions.Image splicing and copy-move are the most common techniques used for creating digital image forgeries. In image splicing, forgery is done by copying a part from one image and pasting to another one. On the other hand, in the copy-move, the copied part is pasted elsewhere in the same image to either add or hide objects. Usually, some processing is done on the copied part either before (e.g. scaling and rotation) or after (e.g. blurring and adding noise) pasting to make the editing less obvious and to eliminate irregularities that could show the image as tampered.The availability of powerful digital image processing programs, such as Photoshop, makes it relatively easy to create digital forgeries from one or multiple images. In a Copy-Move forgery, a part of the image itself is copied and pasted into another part of the same image. This is usually performed with the intention to make an object "disappear" from the image by covering it with a segment copied from another part of the image.

Figure 1.Example image of a typical copy-move forgery. Left: the original image. Right: the tampered image.

Textured areas, such as grass, foliage, gravel, or fabric with irregular patterns, are ideal for this purpose because the copied areas will likely blend with the background and the human eye cannot easily

discern any Suspicious artifacts. Because the copied parts come from the same image,its noise component, and most other important properties will be compatible with the rest of the image and thus will not be detectable using techniques that look for incompatibilities in statistical measures in different parts of the image, and to make the forgery even harder to detect, one can use the available photo editing software's and image processing tools.

II. COPY-MOVE FORGERY DETECTION METHODS

This paper gives survey on various Copy Move Forgery Detection Methods are shown in table 1.

Table 1. Methods of Copy move forgery detection

Sr.no	Title of Paper and Author	Publication	Method	Remark
1.	"An evaluation of popular copy-move forgery detection approaches" by V. Christlein, C. Riess, J. Jordan	IEEE Transaction Information Forensics Security, volume. 7, no. 6, pp. 1841–1854, December 2012.	Block based method is used	Insensitive to low contrast regions also not support low computational load
2.	"Detection of copy-move forgery in digital images" by A. J. Fridrich, B. D. Soukal, and A. J. Lukáš	Proceeding Digit. Forensic Res. Workshop, 2003	Used to detect when the copied area is saved in a lossy format i.e. JPEG	Not perform for the smooth region
3.	"Robust detection of region duplication forgery in digital image" by W. Luo, J. Huang, and G. Qiu	Proceeding 18th International Conference Pattern Recognition (ICPR), volume 4, pp. 746–749, 2006	An efficient and robust algorithm for detecting and localizing this type of malicious tampering.	Advanced computer graphics cannot be detect
4.	"Rotation invariant localization of duplicated image regions based on Zernike moments" by T. Sencar, and N. Memon	IEEE International Conference Acoustic., Speech Signal Process. (ICASSP), Washington, DC, USA, pp. 1053–1056, April 2009	Uses bloom filters for robustness	Advanced computer graphics cannot be detect
5.	"Exposing duplicated regions affected by reflection, rotation and scaling" by S.Bravo-Solorio and A. K. Nandi	Proceeding IEEE International Conference Acoustic , Speech Signal Process. (ICASSP), pp. 1880–1883), May 2011.	Uses color dependent features to reduce the no. of comparison	Very little textural information and work for limited features
6.	"An efficient and robust method for detecting	IEEE Transaction Information Forensics	Based on zernike moments of small	Limitation to the detectors based on

	copy-move forgery" by S.-J. Ryu, M. Kirchner, M.-J. Lee	Security, volume. 8, no. 8, pp. 1355–1370, August. 2013.	image blocks	zernike moments and inherently in capable of localization
7.	"On rotation invariance in copy-move forgery detection" by V. Christlein, C. Riess, and E. Angelopoulou	Proceeding IEEE Workshop International Information Forensics Security. (WIFS), pp.,1–6 December 2010.	Uses block wise feature vectors find similar feature vectors and select pairs that share highly similar shift vector	Involving a rigorous evaluation on the impact of noise and scale invariance SATS
8.	"Image copy-move forgery detection based on SURF" by X. Bo, W. Junwen, L. Guangjie, and D. Yuewei	Proceeding International Conference Multimedia Information Network Security (MINES), pp. 889–892 , November 2010.	Based on SURF also quite robust to additive noise and blurring	Not investigate the automatic locate the tampered region and its boundry
9.	"Region duplication detection using image feature matching" by X. Pan and S. Lyu	IEEE Transaction Information Forensics Security, volume 5, no. 4, pp. 857–867, December 2010.	Only find the duplication region and robust using SURF method	Reliable on the detection of using SIFT keypoints
10.	"Exposing post processed copy–paste forgeries through transform-invariant features" by P. Kakar and N. Sudha	IEEE Transaction Information Forensics Security, volume 7, no. 3, pp. 1018–1028, June 2012.	Invariant features obtained by MPEG-7 image signature tools	Not used for multiply copied detection

III. TYPICAL WORK FLOW FOR COPY MOVE FORGERY DETECTION

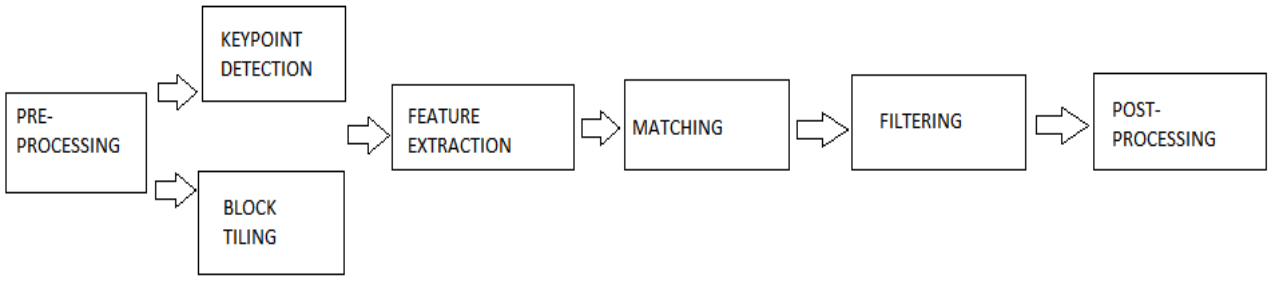

Figure 2.Common processing pipeline for the detection of copy-move forgeries. The feature extraction differs for keypoint-based features (top) and block-based features (bottom).

Although a large number of CMFD methods have beenproposed, most techniques follow a common pipeline, asshown in Fig. 2. Given an original image, there exist two processing alternatives. CMFD methods are either keypointbased methods or block-based methods. In both cases,preprocessing of the images is possible. For instance, mostmethods operate on grayscale images, and as such requirethat the color channels be first merged. For feature extraction, block based methods subdivide the image in rectangularregions. For every such region, a feature vector is computed.Similar feature vectors are subsequently matched. By contrast,keypoint-based methods compute their features only on imageregions with high entropy, without any image subdivision.Similar features within an image are afterwards matched. Aforgery shall be reported if regions of such matches clusterinto larger areas. Both, keypointand block-based methods include further filtering for removing spurious matches. Anoptional postprocessing step of the detected regions may alsobe performed, in order to group matches that jointly follow atransformation pattern.

a) Matching: High similarity between two feature descriptorsis interpreted as a cue for a duplicated region.For block-based methods, most authors propose the use oflexicographic sorting in identifying similar feature vectorsInlexicographic sorting a matrix of feature vectors is built so that every feature vector becomes a row in the matrix. Thismatrix is then row-wise sorted. Thus, the most similar featuresappear in consecutive rows.Other authors use the Best-Bin-First search method derivedfrom the kd-tree algorithm to get approximate nearest neighbors. In particular, keypointbased methodsoften use this approach. Matching with a kd-tree yields a relatively efficient nearest neighbor search. Typically, theEuclidean distance is used as a similarity measure. In priorwork ithas been shown that the use of kd-tree matchingleads, in general, to better results than lexicographic sorting,but the memory requirements are significantly higher. Note, however, that the dimensions of some feature sets are ordered by importance. For thesefeatures, the performance gain over lexicographic sorting isminimal. In our setup we matched feature vectors using the approximate nearest neighbor method. Ituses multiple randomized kd-trees for a fast neighbor search.

b) Filtering: Filtering schemes have been proposed inorder to reduce the probability of false matches. For instance,a common noise suppression measure involves the removal of matches between spatially close regions. Neighboring pixelsoften have similar intensities, which can lead to false forgerydetection. Different distance criteria were also proposed in order to filter out weak matches. For example, several authors proposed the Euclidean distance between matched feature vectors.

c) Postprocessing: The goal of this last step is to onlypreserve matches that exhibit a common behavior. Considera set of matches that belongs to a copied region. These matches are expected to be spatially close to each other in boththe source and the target blocks (or keypoints). Furthermore,matches that originate from the same copy-move action should exhibit similar amounts of translation, scaling and rotation.The most widely used postprocessing variant handles outlier byimposing a minimum number of similar shift vectorsbetween matches. A shift vector contains the translation (inimage coordinates) between two matched feature vectors.Consider, for example, a number of blocks which are simplecopies, without rotation or scaling. Then, the histogram of shift vectors exhibits a peak at the translation parameters ofthe copy operation. Consider a pair of matched featurevectors as forged if: a) they are sufficiently similar, i. e. their Euclidean distance is below a threshold, and b) the neighborhoodaround their spatial locations contains similar features.Anarea threshold can also be applied, so that the detected region has at least a minimum number of points. To handle rotation and scalinguse RANSAC. For a certain number of iterations, a randomsubset of the matches is selected, and

the transformationsof the matches are computed. The transformation which issatisfied by most matches (i. e. which yields most inliers)is chosen.

3.1. Block based Algorithm

We investigated 13 block-based features, which we consideredrepresentative of the entire field. They can be groupedin four categories: moment-based, dimensionality reductionbased,intensity-based, and frequency domain-based features.

Moment-based: We evaluated 3 distinct approaches withinthis class of 24blur-invariant moments as features (BLUR), Hu moments (HU) , Zernike moments(ZERNIKE).

Dimensionality reduction-based: The feature matching space was reduced via principal component analysis (PCA), the Kernel-PCA (KPCA)variant of PCA, also computed the singular valuesof a reduced-rank approximation (SVD). A fourth and Singular Value Decomposition did not yield reliable results in setup and was, thus, excluded from the evaluation.

Intensity-based: The first three features are the average red, green and blue components. Additionally,used directional information of blocks (LUO)while Bravo-Solorioconsider the entropy of a blockas a discriminating feature (BRAVO). Lin (LIN) computed the average grayscaleintensities of a block and its sub-blocks, mean intensities of circles with different radii around the block center (CIRCLE).

Frequency-based: The use of 256coefficients of the discrete cosine transform as features (DCT).The coefficients of a discrete wavelet transform (DWT) usingHaar-Wavelets were recommended the use of the Fourier-MellinTransform (FMT) for generating feature vectors.

3.1.1. Keypoint based Algorithm

Unlike block-based algorithms, keypoint-based methodsrely on the identification and selection of high-entropy imageregions (i. e. the “keypoints”). A feature vector is then extracted per keypoint. Consequently, fewer feature vectors are estimated, resulting in reduced computational complexityof feature matching and post-processing. The lower number of feature vectors dictates that postprocessing thresholds are alsoto be lower than that of block-based methods. A drawback ofkeypoint methods is that copied regions are often only sparselycovered by matched keypoints. If the copied regions exhibitlittle structure, it may happen that the region is completely missed. We examined two different versions of keypointbasedfeature vectors. One uses the SIFT features while theother uses the SURF features. They are denoted asSIFT and SURF, respectively. The feature extraction is implementedin standard libraries. However, particular differencesof keypoint-based algorithms lie in the postprocessing of thematched features.

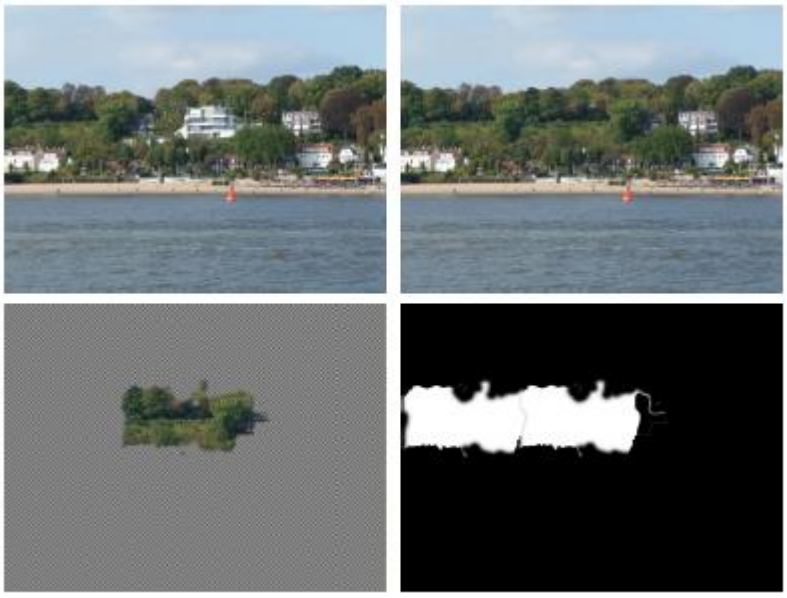

Figure 3.The image beachwood (upper left) is forged with a green patch (bottom left) to conceal a building (upper right). A ground truth map (bottom right) is generated where copy-moved pixels are white, unaltered pixels are black and boundary pixels are gray.

IV. CONCLUSION

Akeypoint-based method, e. g. based on SIFT features, can be very efficiently executed. its mainadvantage is the remarkably low computational load, combinedwith good performance. Keypointbased methods, however,are sensitive to low-contrast regions and repetitive image content. Here, block-based methods can clearly improve the detection results. In a number of experiments, five block-basedfeature sets stood out, namely DCT, DWT, KPCA, PCA andzernike. Among thesewe recommend the use of ZERNIKE,mainly due to its relatively small memory footprint.

REFERENCES

1. V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," IEEE Transaction Information Forensics Security, volume. 7, no. 6, pp. 1841–1854, December 2012.
2. A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, "Detection of copy-move forgery in digital images," in Procedure. Digit. Forensic Res. Workshop, 2003.
3. W. Luo, J. Huang, and G. Qiu, "Robust detection of region duplication forgery in digital image," in Procedure. 18th International Conference Pattern Recognition (ICPR), volume 4, pp. 746–749, 2006.
4. S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in Procedure IEEE International Conference Acoustic., Speech Signal Process. (ICASSP), Washington, DC, USA, pp. 1053–1056, April 2009.
5. S.Bravo-Solorio and A. K. Nandi, "Exposing duplicated regions affected by reflection, rotation and scaling," in Procedure IEEE International Conference Acoustic , Speech Signal Process. (ICASSP), pp. 1880–1883), May 2011.
6. S.-J. Ryu, M. Kirchner, M.-J. Lee, and H.-K. Lee, "Rotation invariant localization of duplicated image regions based on Zernike moments," IEEE Transaction Information Forensics Security, volume. 8, no. 8, pp. 1355–1370, August. 2013.
7. V. Christlein, C. Riess, and E. Angelopoulou, "On rotation invariance in copy-move forgery detection," in Procedure IEEE Workshop International Information Forensics Security. (WIFS), pp.,1–6 December 2010.

8. X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, "Image copy-move forgery detection based on SURF," in Procedure International Conference Multimedia Information Network Security (MINES), pp. 889–892 , November 2010.
9. X. Pan and S. Lyu, "Region duplication detection using image feature matching," IEEE Transaction Information Forensics Security, volume 5, no. 4, pp. 857–867, December 2010.
10. P. Kakar and N. Sudha, "Exposing post processed copy–paste forgeries through transform-invariant features," IEEE Transaction Information Forensics Security, volume 7, no. 3, pp. 1018–1028, June 2012.
11. D. G. Lowe, "Distinctive image features from scale-invariant keypoints," International Journal Computional Visual, volume 60, no. 2, pp. 91–110, November 2004.
12. H. Bay, A. Ess, T. Tuytelaars, and L. Van Gool, "SURF: Speeded up robust features," Computional Visual Image Understand, volume 110, no. 3, pp. 346–359, June 2008.
13. M. A. Fischler and R. C. Bolles, "Random sample consensus: A paradigm for model fitting with applications to image analysis and automated cartography," Communication ACM, volume 24, no. 6, pp. 381–395, June 1981.
14. M. Bronstein and M. M. Bronstein, "Not only size matters: Regularized partial matching of nonrigid shapes," in Procedure IEEE Computational Society Conference Computational Visual Pattern Recognition Workshop (CVPRW, pp. 1–6), June 2008.
15. D. R. Martin, C. C. Fowlkes, and J. Malik, "Learning to detect natural image boundaries using local brightness, color, and texture cues," IEEE Transaction Pattern Analysis Machine Intelligence, volume 26, no. 5, pp. 530–549, May 2004.

