Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Engineering

Elixir Comp. Engg. 117 (2018) 50389-50391

ISSN: 2229-712X

Digital Image Forgery Detection Using Passive Techniques by Means of Keypoint Classification

Sonal P. Patil and K. N. Jariwala
Department of Computer Engineering, S.V.N.I.T, Surat, India.

ARTICLE INFO

Article history:
Received: 1 March 2018;
Received in revised form:
27 March 2018;
Accepted: 7 April 2018;

Keywords
Image forensics,
Copy-move forgery,
Dataset,
Manipulation detection,
Comparative study.

ABSTRACT
In today's era manipulation of image has become a simple task because of advanced photo editing software packages as well as the capturing devices having high resolution. Verification of the truthfulness of images as well as detection of tampering without having the extra prior knowledge of image content is a significant research field. An attempt is made to review the recent developments in digital image forgery detection. Passive methods do not require prior information about the image. In this paper first various image forgery detection techniques are classified and then its general structure is developed. Passive image authentication overview is presented and the existing passive forgery detection techniques are reviewed. The present status of image forgery detection technique is discussed along with a recommendation for future research. In this paper the effort has been made for finding the best forgery detection algorithm such as SIFT for identifying the manipulated region. The common scenario has been considered where the goal is to remove the features. The attacks conceived so far against SIFT-based forensic techniques implicitly assume that all SIFT keypoints have similar properties. It is better to use SIFT classification scheme based on the gray scale histogram of the neighborhood of SIFT keypoints.

1. Introduction

Now a day's Image forensics has become important research topic as it is necessary to study the methods which give the wrong impression by concealing traces of manipulations [1].This respective discipline has already turn into a standard for image forensic techniques security whose correct behaviors may be intentionally hindered by an adversary (or attacker) who is interested on covering traces of malicious tampering. Nowadays, it is possible to conceal traces of contrast enhancement, compression or resampling [2-4]. In [1], two categorizations of counter-forensic schemes (or attacks) are proposed: in the image acquisition chain an attack takes place (integrated or post-processing i.e., during or after the acquisition) and the attacker is having knowledge about countered forensic algorithm. Regardless of its category an attack should respect some constraints while attempting to mislead a certain forensic technique, such as preserving the visual quality of the forged image and the integrity of the semantic message conveyed by the content.

A part of the image is copied and then pasted at one or many times into same image or other image which is the common technique of manipulating the similarity content of the image which is called as image forgery.Generally similar semantic as well as statistical properties are shared by the original and forged images.Such similarities can be used to identify the manipulated area. In recent era more number of copy move detectors are explained which are basically classified into two categories i.e.block based methods and key points based methods.In previous methods the image is divided into various overlapping blocks and then the same features should be extracted which are used for matching the similar blocks [6, 7]. The methods are used for extracting the highest descriptive robust points of an image and univocal features vector is assigned to each. Those vectors are used for matching the similar points within images. Within these methods, scale invariant feature transform(SIFT) and methods based on SIFT are current methods and very effective in nature [10].SIFT is well capable to identify the correspondences in between the visual contents which are similar rather it has been allowed for detecting the accurate and real forgery.The robustness of various detectors is considered by Chrislein et al. [11]. They have observed that the block based methods are not much strong against the resampling,noise and compression.Three block based detectors are impaired by combining the manipulations by Nguyen et al. [12]. It is essential to understand the security of SIFT algorithm. The first study in this direction is the one by Hsu et al. [13] has proposed the analysis of simple attacks after that the method has been analyzed to strengthen key points of SIFT.Subsequent to this work Do et al.[14-16] payed attention on a SIFT-based content-based image retrieval (CBIR) [17] scenario and invented a number of interesting attacks. The aim of the previous works is to modify the SIFT feature descriptor of key points but they do not consider the complete removal of the key points.An attack which is based on the local wrapping techniques are derived in the work [18].All the studies carried out so far have demonstrated that devising methods to attack SIFT features is not a trivial task. SIFT features are robust not only against several non malicious processing but also against tampering attempts. Most attacks in fact pay a high cost in terms of visual quality degradation.

New keypoints are created for the purpose of removing SIFT keypoints. SIFT analysis has been applied to each and every key points of an image. The methods which are used for countering the SIFT based analysis are applied to all the keypoints of an image.

In this paper the methods that improve the performance of existing approaches are discussed. It is possible to discriminate between SIFT keypoints and to plan attacks that are used for the modification of the characteristics of the keypoints

2. SIFT-based COPY MOVE forgery detection

In this section the SIFT techniques has been reviewed and the techniques based on copy move detectors are explained.

2.1 Scale invariant feature transform

Due to robustness to clutter, geometric transformations and occlusion now a day's SIFT features are very popular in applications of pattern recognition [10].The inspiration behind this kind of visual local features is to model a complex object or a scene by a collection of salient points.

SIFT features of an image are detected at various scales by taking help of a scale-space representation which is implemented as an image pyramid in a nutshell. By using Gaussian smoothing and sub sampling the pyramid levels are obtained whereas the interest points are chosen as local min or max in the scale space. The numerous candidate keypoints are produced by the detection of min max i.e. extreme. Generally robustness is not produced by all the candidates and thus need of discrimination is occurred. So SIFT algorithm performs the checks against the various thresholds. The common values were set by Lowe in [10].

The first check verifies whether the contrast value of the keypoints neighborhood is sufficiently large or not. While the second check is responsible to verify the keypoint is isolated enough from an image edge.The candidate keypoint is rejected if the either of any check fails.

The real keypoint falls below the thresholds i.e. false negative or any forged keypoint is raised above any threshold is nothing but alteration of an image. The keypoints that passed both the previous tests guarantee invariance to scaling and affine transformations.

The algorithm allocates canonical orientation to each of them to guarantee rotation invariance. By using means of a histogram of gradient orientations computed in the neighbor hood of the keypoints descriptor i.e.unique fingerprint is computed in order to recognize univocally a keypoint. Therefore, a SIFT keypoint is completely described by the following information xi ={x, y, σ, o, f},where(x, y)are the coordinates in the image plane, σ is the scale of the keypoint, o is the canonical orientation and f is the final SIFT descriptor

2.2 Copy-move detection

The SIFT operator is applied to two images in pattern recognition i.e. a target and a test image. The SIFT operator is applied to only one image in copy move forgery detection. In fact the copied part is seen in the same image as shown in figure 1. The keypoints extracted in the region will be almost similar to the original hence matching between SIFT features can be utilized for discovering the part which was copied and geometric transformation was applied. In this era different techniques are proposed for addressing the problem of copy move forgery detection in digital images. The image is divided into overlapping blocks and after that it extracts some peculiar features which reveal whether some of the blocks are duplicated or not [5].

A decision about forgery is made which is depending on the amount of characteristics of the paired blocks. Such methods are not robust against rotation and scaling operations in copy move forgeries.The various SIFT features used to allow to overcome the limitations of fundamental robustness against transformations. The most interested SIFT based copy move detection technique is the one which is proposed by Amerini et al.[9],this respective technique is able for detecting and estimating the geometric transformation which is applied in a copy move forgery attack.A clustering procedure is utilized for improving the accuracy this is the idea for the presence of cloned areas.

To understand whether an area has been cloned or not an agglomerative hierarchical clustering is performed on spatial locations, i.e., (x, y) coordinates of the matched points. Such method creates a hierarchy of clusters which can be represented by means of a tree structure.

The working of clustering algorithm is as follows

1. Each and every keypoint is assigned to a cluster.
2. The computation of reciprocal spatial distances among clusters is computed.
3. The closest pair of clusters if found.
4. The acquired pair is merged into a single cluster.

Accordingly if two or more clusters are detected with at least four pair of matched points then they can be linked to a cluster with another cluster and then the matching regions are considered for cloning.The method can decide which geometric transformation can be used and applied in between the main original region and copy move region by using homography.

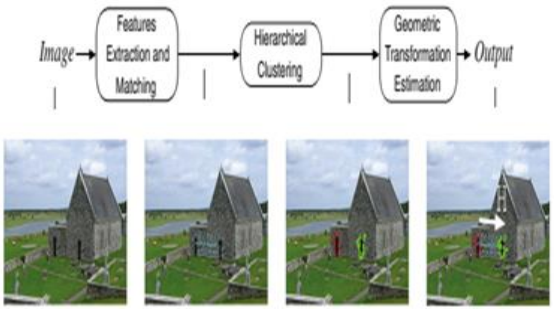

Figure 1. Overview of the method SIFT matched pairs and clustering [9].

3. Classification of SIFT keypoints

In this section the classification method is described, then classes are defined and then some visual examples of classes are given.

3.1 The rationale behind the classification

In standard, we would visualize that the categorization relies on the visual content surrounding the keypoints. Analyzing the gray scale histogram of every small region surrounding the keypoint has been chosen though the task can be performed by using number of ways like textures, edges, shapes etc.

The number of modes can be chosen as the valuable information about the local image which can be provided among all the characteristics of an image histogram. The idea is that the effectiveness of an attack may be strictly related to the properties of the keypoint we attempt to remove.

As an instance, assume that the neighborhood of a keypoints contains a straight vertical edge; so the local warping attack which is stated [18], would probably succeed in deleting it. But after the attack takes place unfortunately the edge will not be straight anymore and the bending effect will be clearly visible.

A Gaussian smoothing attack may be used to delete the keypoint perhaps with a considerably lower impact on the quality. The assumption is that the working will be on gray scale images and the consideration of SIFT keypoints are originated by the first scale of the image i.e. s=0. The reason behind the later assumption is as follows.

1)The keypoints of the region of the first octave is more difficult to remove.

2)For getting clarity the significant keypoints are considered in spite of excessive amount of keypoints.

The experimental analysis has been carried out on two distinct sets of images. To demonstrate the effectiveness of our technique and its robustness against different SIFT implementations the UCID database has been used [21]. Such data set which is a well-known benchmark amongst the image retrieval research community consists of 1,338 uncompressed (TIFF)color images with contents depicting landscapes, cityscapes, people and man-made objects.The huge collection gives permission to make conclusive statements on the performance of the technique.Set of 10 images are used which contains a realistic copy move forgery to demonstrate the capability of the method to impair a SIFT based copy move detector.

4. Conclusion

In this paper, a counter-forensic scheme has been discussed to counter a SIFT-based copy-move detector. The goal is to remove SIFT keypoints with the lowest possible impact on visual quality. To do so, first classification of SIFT keypoints depending on the histogram of their neighborhood has been done. Then an attack has been used specifically to tailor to each class. Results will be better than those obtained by always using the same attack regardless of keypoints properties. Several aspects could be further investigated, the most interesting of which is the injection of fake keypoints into the cleaned image. In fact, an image that does not contain SIFT keypoints (or very few of them) is suspicious: such absence could be taken as a clue of tampering, thus leading to a counter detector with a very straight forward imple mentation. As a matter of fact, in a copy-move scenario, the side effect of the classification-based attack tends to be less noticeable,mainly for two reasons:(1) only half of the keypoints are removed from each patch and (2)some keypoints are actually not removed but altered in such a way that their previous match is canceled .Moreover, it could be useful to study more in depth the interactions between the countermeasures against SIFT-based and block-based copy-move detectors. Finally, it would also be interesting to apply attack to a content-based image retrieval scenario in order to assess its effectiveness against SIFT-based search engines.

References

[1]. Amerindian al., “Counter-forensics of SIFT-based copy move detection by means of keypoint classification”, EURASIP Journal on Image and Video Processing 20132013:18.

[2]. G Cao, Y Zhao, R Ni, H Tian, “ Anti-forensics of contrast enhancement in digital images”,in Proceedings of the 12th ACM Workshop on Multimedia and Security (ACM, New York, 2010), pp. 25–34

[3]. M Stamm, S Tjoa, W Lin, K Liu, “Undetectable image tampering through JPEG compression anti-forensics” , 17th IEEE International Conference on Image Processing (ICIP) (IEEE, New York, 2010), pp. 2109–2112

[4]. M Kirchner, R Bohme, “Hiding traces of resampling in digital images”, IEEE Trans. Inf. Forensics Security.3 (4), 582–592 (2008)

[5]. S Bayram, H Sencar, N Memon,“A survey of copy-move forgery detection techniques”, in IEEE Western New York Image Processing Workshop. (IEEE, New York, 2008), pp. 538–542

[6]. A Fridrich, B Soukal, A Luk,“Detection of copy-move forgery in digital images” in Proceedings of Digital Forensic Research Workshop

[7]. H Popescu, AC Farid, “Exposing digital forgeries by detecting traces of resampling”, IEEE Trans. Signal Process 53(2), 758–767 (2005)

[8]. X Pan, S Lyu,“Region duplication detection using image feature matching”, IEEE Trans. Information Forensics and Security. 5(4), 857–867 (2010)

[9]. I Amerini, L Ballan, R Caldelli, A Del Bimbo, G Serra, “A SIFT-based forensic method for copy move attack and transformation recovery”, IEEE. Trans. Information Forensics Security 6(3), 1099 –1110 (2011)

[10]. DG Lowe, “Distinctive image features from scale-invariant keypoints”, Int. J. Comput. Vis.60 (2), 91–110 (2004)

[11]. V Christlein,C Riess, J Jordan,C Riess,E Angelopoulou, “An evaluation of popular copy-move forgery detection approaches”, IEEE. Trans. Signal Process, 1841–1854 (2012)

[12]. S Nguyen, HC Katzenbeisser, “Security of copy-move forgery detection techniques”, IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). (IEEE, New York, 2011), pp. 1864 –1867

[13]. SC Hsu, CY Lu, CS Pei, “Secure and robust SIFT”, in Proceedings of the 17th ACM International Conference on Multimedia (ACM, New York, 2009),pp. 637–640

[14]. E Do, TT Kijak,T Furon, L Amsaleg, in Proceedings of the International Conference on Multimedia. “Understanding the security and robustness of SIFT” (ACM, New York, 2010), pp. 1195–1198

[15]. E Do, TT Kijak, T Furon, L Amsaleg, “Deluding image recognition in sift-based CBIR systems” , in Proceedings of the 2nd ACM Workshop on Multimedia in forensics, Security and Intelligence. (ACM, New York, 2010), pp. 7–12

[16]. E Do, TT Kijak, L Amsaleg, T Furon, “Enlarging hacker’s toolbox: deluding image recognition by attacking keypoint orientations” in 37th International Conference on Acoustics, Speech, and Signal Processing, ICASSP’12. (IEEE, New York, 2011)

[17]. Y Liu, D Zhang, G Lu, W Ma,“A survey of content-based image retrieval with high-level semantics”,IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 262–282 (2007)

[18]. R Caldelli, I Amerini, L Ballan, G Serra, M Barni, A Costanzo,“On the effectiveness of local warping against SIFT-based copy-move detection”in Proceedings of International Symposium on Communications, Control and Signal Processing (ISCCSP).(IEEE, New York, 2012)